University of Cambridge

TRINITY COLLEGE

Doctoral Thesis

Computing the Cassels-Tate Pairing for Jacobian Varieties of Genus Two Curves

Author:
Jiali Yan

Supervisor:
Dr. Tom Fisher

This thesis is submitted for the degree of Doctor of Philosophy

in the

Department of Pure Mathematics and Mathematical Statistics

March 2021

Declaration of Authorship

This thesis is the result of my own work and includes nothing which is the outcome of work done in collaboration except as declared in the Preface and specified in the text. It is not substantially the same as any that I have submitted, or, is being concurrently submitted for a degree, diploma or other qualification at the University of Cambridge or any other University or similar institution except as declared in the Preface and specified in the text. I further state that no substantial part of my dissertation has already been submitted, or, is being concurrently submitted for any such degree, diploma or other qualification at the University of Cambridge or any other University of similar institution except as declared in the Preface and specified in the text. It does not exceed the prescribed word limit.

Signed: Jiali Yan

Date: March, 2021

Abstract

Title: Computing the Cassels-Tate Pairing for Jacobian Varieties of Genus Two Curves

Author: Jiali Yan

Let J be the Jacobian variety of a genus two curve defined over a number field K. The main focus of this thesis is on computing the Cassels-Tate pairing on the 2-Selmer group of J.

We start by studying the Cassels-Tate pairing when J admits a Richelot isogeny $\phi : J \to \widehat{J}$. Suppose all points in $J[2]$ are defined over K. We compute the Cassels-Tate pairing $\langle\ ,\ \rangle_{CT}$ on $\mathrm{Sel}^{\widehat{\phi}}(\widehat{J}) \times \mathrm{Sel}^{\widehat{\phi}}(\widehat{J})$ following the Weil pairing definition of the Cassels-Tate pairing.

We then study the pairing $\langle\ ,\ \rangle_{CT}$ on $\mathrm{Sel}^2(J) \times \mathrm{Sel}^2(J)$ following the homogeneous space definition of the Cassels-Tate pairing. For $\epsilon, \eta \in \mathrm{Sel}^2(J)$, we compute $\langle \epsilon, \eta \rangle_{CT}$ both in the case where all points in $J[2]$ are defined over K and in the case where the twisted Kummer surface $\mathcal{K}_\eta$ has a K-rational point. In both cases, we give a computable formula for $\langle \epsilon, \eta \rangle_{CT}$ and a practical algorithm for computation when $K = \mathbb{Q}$.

In all cases, we calculate examples for which computing the Cassels-Tate pairing improves the rank bound of J obtained by carrying out standard descent calculations. We also give techniques to reduce the degree of the number field needed in the algorithm for computation.

Acknowledgements

First of all, I would like to express my sincere and deepest gratitude to my supervisor, Dr. Tom Fisher, for his patient guidance and insightful comments at every stage during my research. I am grateful to Trinity College and the Department of Pure Mathematics and Mathematical Statistics for their financial support.

I would also like to thank my husband, Yanning Xu, for his support throughout all these years. I thank my office mates Lazar Radičević and Yanning Xu for many interesting mathematical conversations. Finally, I would like to thank my parents for their encouragement and understanding.

Contents

Introduction

Let A be an abelian variety defined over a number field K. The Mordell-Weil Theorem tells us that $A(K)$, the set of K-rational points on A, is a finitely generated abelian group. This implies that the rank of $A(K)$, denoted by $r(A)$, is finite. However, computing $r(A)$ can be difficult and in fact there is no known algorithm to do this. Methods have been developed to compute upper bounds on $r(A)$. One standard method, known as a descent calculation, follows the proof of the Mordell-Weil Theorem and computes the Selmer groups of A. The n-Selmer group of A, denoted by $\mathrm{Sel}^n(A)$, consists of all the isomorphism classes of the n-coverings of A that have points everywhere locally. Computing $\mathrm{Sel}^n(A)$ gives an upper bound on $r(A)$ because $r(A)$ can be bounded in terms of $|A(K)/nA(K)|$ for $n \geq 2$ and we have the following exact sequence

$$0 \to \frac{A(K)}{nA(K)} \to \mathrm{Sel}^n(A) \to Ш(A)[n] \to 0,$$

which involves $Ш(A)$, the Tate-Shafarevich group of A. The Tate-Shafarevich group is first introduced by Lang, Tate and Shafarevich in [LT58] [Sha59]. This group consists of all the isomorphism classes of principal homogeneous spaces of A that have points everywhere locally and is conjectured to always be finite. The study of $Ш(A)$ is key in the understanding of the arithmetic of A. In the problem of bounding the rank, the discovery of any nontrivial element in $Ш(A)[n]$ improves the upper bound on $r(A)$.

One important feature of the Tate-Shafarevich group is the existence of the Cassels-Tate pairing. In [Cas59] [Cas62], Cassels proved that for an elliptic curve E defined over a number field, there exists a pairing

$$Ш(E) \times Ш(E) \to \mathbb{Q}/\mathbb{Z},$$

that is nondegenerate after quotienting out the maximal divisible subgroup of $Ш(E)$. He also proved that this pairing is alternating. If $Ш(E)$ is finite, which is conjectured to always be the case, then this implies that the order of $Ш(E)$ is a square. In [Tat62], Tate generalized these results and showed that for an abelian variety A, with $A^\vee$ denoting its dual, there is a pairing

$$Ш(A) \times Ш(A^\vee) \to \mathbb{Q}/\mathbb{Z},$$

that is nondegenerate after quotienting out the maximal divisible subgroups. In the same paper, Tate also showed the alternating property in the case where $Ш(A)$ is mapped to $Ш(A^\vee)$ via a polarization induced by a K-rational divisor on A. In [Fla90], Flach proved that for principally polarized abelian varieties,

the pairing is always antisymmetric. The pairing was believed to always be alternating for principally polarized abelian varieties until Poonen and Stoll gave explicit counterexamples and showed that the order of $Ш(A)$ need not be a square even in the case where A is Jacobian variety of a curve defined over $\mathbb{Q}$ in [PS99].

This pairing is called the Cassels-Tate pairing and it natually lifts to a pairing on Selmer groups. One application of this pairing is in improving the bound on $r(A)$ obtained by performing a standard descent calculation. More specifically, if $Ш(A)$ is finite for a principally polarized abelian variety A, the kernel of the Cassels-Tate pairing on $\mathrm{Sel}^n(A) \times \mathrm{Sel}^n(A)$ is equal to the image of the natural map $\mathrm{Sel}^{n^2}(A) \to \mathrm{Sel}^n(A)$ induced from the map $A[n^2] \xrightarrow{n} A[n]$, see Proposition 1.9.3 for details. This shows that carrying out an n-descent and computing the Cassels-Tate pairing on $\mathrm{Sel}^n(A) \times \mathrm{Sel}^n(A)$ gives the same rank bound as obtained from n^2-descent where $\mathrm{Sel}^{n^2}(A)$ needs to be computed.

There have been many results on computing the Cassels-Tate pairing in the case of elliptic curves. For example, in addition to defining the pairing, Cassels also described a method for computing the pairing on $\mathrm{Sel}^2(E) \times \mathrm{Sel}^2(E)$ in [Cas98] by solving conics over the field of definition of a two-torsion point. Donnelly [Don15] then decribed a method that only requires solving conics over K and Fisher [Fis16] used the invariant theory of binary quartics to give a new formula for the Cassels-Tate pairing on $\mathrm{Sel}^2(E) \times \mathrm{Sel}^2(E)$ without solving any conics. In [vB] [vBF18], van Beek and Fisher computed the Cassels-Tate pairing on the 3-isogeny Selmer group of an elliptic curve. For $p = 3$ or 5, Fisher computed the Cassels-Tate pairing on the p-isogeny Selmer group of an elliptic curve in a special case in [Fis03]. In [FN14], Fisher and Newton computed the Cassels-Tate pairing on $\mathrm{Sel}^3(E) \times \mathrm{Sel}^3(E)$.

The natural problem is to generalize the different algorithms for computing the Cassels-Tate pairing for elliptic curves to compute the pairing for abelian varieties of higher dimension. Let J be the Jacobian variety of a genus two curve $\mathcal{C}$ defined over a number field K. In this thesis, we will mainly be computing the Cassels-Tate pairing on $\mathrm{Sel}^2(J) \times \mathrm{Sel}^2(J)$. The methods we give for computing the pairing in theory work over any number field K but in practice, we have only computed examples when $K = \mathbb{Q}$.

In Chapter 1, we state some basic definitions and preliminary theory needed for the other chapters. In [PS99], four definitions of the Cassels-Tate pairing for an abelian variety were given and proved to be equivalent. In this thesis, we will follow the Weil pairing definition and the homogeneous space definition of the Cassels-Tate pairing.

In Chapter 2, we study the Cassels-Tate pairing on Jacobians of genus two curves admitting a special type of isogenies called Richelot isogenies. Suppose there exists a Richelot isogeny $\phi : J \to \widehat{J}$. Similar to the elliptic curve case, we define a pairing on $\mathrm{Sel}^\phi(J) \times \mathrm{Sel}^\phi(J)$ which is shown to be compatible with

the Cassels-Tate pairing on $\mathrm{Sel}^2(J) \times \mathrm{Sel}^2(J)$ following the Weil pairing definition of the Cassels-Tate pairing. We then give an algorithm to compute the Cassels-Tate pairing on $\mathrm{Sel}^{\widehat{\phi}}(\widehat{J}) \times \mathrm{Sel}^{\widehat{\phi}}(\widehat{J})$ where $\widehat{\phi}$ is the dual isogeny of ϕ. The algorithm is under the assumption that all two-torsion points on J are defined over K. We end this chapter with a worked example. This example demonstrates we can turn the descent by Richelot isogeny into a 2-descent via computing the Cassels-Tate pairing.

In Chapter 3, we describe two different methods for computing the linear isomorphism between the Kummer surface, which is the quotient of J by the involution $[-1]$, and the twisted Kummer surface, which is the quotient by the induced involution of a 2-covering of J corresponding to a Selmer element. This also gives the defining equation of the twisted Kummer surface. We give an algorithm to trivialize a matrix algebra over $\mathbb{Q}$ given the structure constants, with the precise statement of the problem described in Problem 3.4.1. This is an important step in computing the twist map and is useful in the later algorithms for computing the Cassels-Tate pairing.

In Chapter 4, we prove a new algorithm that explicitly computes the Cassels-Tate pairing on $\mathrm{Sel}^2(J) \times \mathrm{Sel}^2(J)$, with the assumption that all the two-torsion points on J are defined over K. This algorithm follows the homogeneous space definition of the Cassels-Tate pairing. We demonstrate by a worked example how this algorithm can potentially improve the rank bound of J obtained from performing a 2-descent calculation. In fact, in the case where all points in $J[2]$ are defined over K, computing the Cassels-Tate pairing on $\mathrm{Sel}^2(J) \times \mathrm{Sel}^2(J)$ gives the same rank bound as obtained from carrying out a 4-descent which requires computing $\mathrm{Sel}^4(J)$. We also prove a formula for the obstruction map $\mathrm{Ob} : H^1(G_K, J[2]) \to \mathrm{Br}(K)$ which generalizes the work of Clark and O'Neil in the elliptic curve case.

In Chapter 5, we prove a new algorithm for explicitly computing the Cassels-Tate pairing on $\mathrm{Sel}^2(J) \times \mathrm{Sel}^2(J)$, with no more conditions on the two-torsion points of J but rather the condition that the twisted Kummer surfaces have K-rational points. The method follows the homogeneous space definition of the Cassels-Tate pairing and is a generalization of the results in [Fis16] in the elliptic curve case. We also include a worked example that demonstrates the improvement of the rank bound of J obtained from performing a 2-descent calculation. However, this algorithm requires calculations in a large degree number field in the most general case. Therefore it is more practical when the Galois group of $f(x)$ is relatively small where the genus two curve is defined by $y^2 = f(x)$. For this reason, new computing techniques are developed to improve the algorithm and they are explained in the final chapter of the thesis.

In Chapter 6, we improve the algorithm in Chapter 5. The result of the improvement is that we can now compute the Cassels-Tate pairing with the assumption that the twisted Kummer surfaces have K-rational points in the most general case with the precise condition given at the end of Section 6.2.1. We

also end this chapter with a worked example where computing the Cassels-Tate pairing improves the rank bound of J obtained from carrying out a 2-descent calculation.

Chapter 1

Background and Preliminary Results

In this chapter, we will state some useful definitions and preliminary results needed for the later chapters.

1.1 Notation

This section gives some basic definitions and notation used throughout this thesis.

Unless stated otherwise, we are working over K, a perfect field with characteristic not equal to $2, 3,$ or 5. For any field K, we let $\bar{K}$ denote its algebraic closure and let $\mu_n \subset \bar{K}$ denote the n^{th} roots of unity in $\bar{K}$. We let G_K denote the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$ and let $G_{L/K}$ denote $\mathrm{Gal}(L/K)$ for L a Galois extension of K. All algebras in this thesis are assumed to be associative. For a K-algebra A, $\mu_n(A) \subset A$ denotes the n^{th} roots of unity in A. For a finite dimensional K-algebra A, we let $N_{A/K} : A \to K$ denote the norm map and we sometimes abbreviate $N_{A/K}$ to N when the context is clear. A local field in this thesis is always isomorphic to a finite extension of the p-adic numbers $\mathbb{Q}_p$ where p is a prime number, unless stated otherwise.

Suppose A, B are two K-algebras or two varieties defined over K. Let L be a field extension of K. Sometimes we write A over L to mean $A \otimes_K L$ or A_L and $A \cong B$ over L to mean $A \otimes_K L \cong B \otimes_K L$ or $A_L \cong B_L$ with the isomorphism defined over L. For a variety A defined over K, we sometimes abbreviate $A(\bar{K})$ to A when the context is clear.

A general *genus two curve* $\mathcal{C}$ defined over K is a smooth projective curve and it can be given in the following hyperelliptic form:

$$\mathcal{C} : y^2 = f(x) = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0,$$

where $f_i \in K$, $f_6 \neq 0$ and the discriminant $\triangle(f) \neq 0$, which implies that f has distinct roots in $\bar{K}$.

We define the *Weierstrass points* of $\mathcal{C}$ to be the points on $\mathcal{C}$ with the y-coordinate being 0 and denote *the points at infinity* by ∞^+, ∞^-. The curve is reducible to the form of y^2 equal to a quintic in x if and only if the original sextic f has a rational root. In the case where f is reduced to a quintic, we denote the unique point at infinity by ∞. Note in this case, ∞ is also a Weierstrass point. Alternatively, the Weierstrass points of a hyperelliptic curve are defined to be the ramification locus of the degree two morphism from the curve to $\mathbb{P}^1$ where $(x, y) \mapsto x$. We note the involution on $\mathcal{C} : (x, y) \mapsto (x, -y)$.

1.2 The Jacobian Variety and Its Kummer Surface

This section states some definitions and properties of the Jacobian variety of a genus two curve.

1.2.1 Picard group

We define the *Picard group* of a general genus two curve $\mathcal{C}$, denoted by $\mathrm{Pic}(\mathcal{C})$, to be the group of divisor classes of $\mathcal{C}$, that is the group of divisors of $\mathcal{C}$ modulo linear equivalence. Then $\mathrm{Pic}^d(\mathcal{C})$ denotes the elements in $\mathrm{Pic}(\mathcal{C})$ of degree d. The *canonical divisor class* of $\mathcal{C}$, denoted by $K_{\mathcal{C}}$, is the divisor class $[\infty^+ + \infty^-]$. Via the natural isomorphism $\mathrm{Pic}^2(\mathcal{C}) \to \mathrm{Pic}^0(\mathcal{C})$ sending $[P_1 + P_2] \mapsto [P_1 + P_2 - \infty^+ - \infty^-]$, it is convenient to represent any element of $\mathrm{Pic}^0(\mathcal{C})$ by an unordered pair of points $\{P_1, P_2\}$ on $\mathcal{C}$ as it corresponds to $[P_1 + P_2 - \infty^+ - \infty^-] \in \mathrm{Pic}^0(\mathcal{C})$. Using the Riemann-Roch Theorem, this representation is unique if we identify all pairs in the form $\{(x, y), (x, -y)\}$ along with $\{\infty^+, \infty^-\}$ to give the identity element in $\mathrm{Pic}^0(\mathcal{C})$.

1.2.2 Jacobian variety

The *Jacobian variety* of a genus two curve $\mathcal{C}$ defined over K, denoted by J, is an abelian variety of dimension 2 defined over K which can be identified with $\mathrm{Pic}^0(\mathcal{C})$. We denote the identity element of J by $\mathcal{O}_J$. From Section 1.2.1, we know that a point $P \in J$ can be identified with an unordered pair of points of $\mathcal{C}$, $\{P_1, P_2\}$. This identification is unique unless $P = \mathcal{O}_J$, in which case it can be represented by any pair of points on $\mathcal{C}$ in the form $\{(x, y), (x, -y)\}$ or $\{\infty^+, \infty^-\}$. It is well known that that there exists a birational morphism from $\mathrm{Sym}^2\mathcal{C}$ to J given by the identification above, where $\mathrm{Sym}^2\mathcal{C}$ denotes the quotient of $\mathcal{C} \times \mathcal{C}$ by the equivalence relationship $(Q_1, Q_2) \sim (Q_2, Q_1)$.

In this thesis, we let τ_P denote the translation by P on J, for any $P \in J$. We give the following remark to describe the two-torsion points on J.

Remark 1.2.1. Suppose $\mathcal{C}$ is defined by $y^2 = f(x)$ with the roots of f denoted by $\omega_1, ..., \omega_6$. The point $P \in J$ is a two-torsion point if P corresponds to $\{P_1, P_2\}$ and P_1, P_2 are Weierstrass points of $\mathcal{C}$. It is known that $|J[2]| = 16$, and we will normally denote $J[2]$ by $\{\mathcal{O}_J, \{(\omega_i, 0), (\omega_j, 0)\}$ for $i \neq j\}$. In the case where the curve is reduced to the form where f is degree 5 with roots $\omega_1, ..., \omega_5$, $J[2] = \{\mathcal{O}_J, \{(\omega_i, 0), (\omega_j, 0)\}$ for $i \neq j, \{(\omega_i, 0), \infty\}\}$.

The group law

We describe the group law on J generically as in [CF96, Chapter 1 Section 2]. Let $\{(x_1, y_1), (x_2, y_2)\}, \{(u_1, v_1), (u_2, v_2)\}$ represent two general points $P, Q \in J$ defined over K. There is a unique $M(x) \in K[x]$ of degree 3 such that $y = M(x)$ passes through the 4 points on $\mathcal{C}$. The intersection of the cubic curve with $\mathcal{C}$, given by $M(x)^2 = f(x), Y = M(x)$, gives two other points on $\mathcal{C}$ also defined over K which represent $R \in J$. Then $P + Q + R = \mathcal{O}_J$. This defines the group law on J.

1.2.3 Theta divisor

In this thesis, the *theta divisor*, denoted by Θ, is defined to be the divisor on J that corresponds to the divisor $\{P\} \times \mathcal{C} + \mathcal{C} \times \{P\}$ on $\mathcal{C} \times \mathcal{C}$ under the birational morphism $\mathrm{Sym}^2\mathcal{C} \to J$, for some point $P \in \mathcal{C}$. We sometimes also denote it by Θ_P in order to show the choice of the point P. In this thesis, we always pick P to be one of the Weierstrass points for Θ, unless stated otherwise. We have the following useful facts about the theta divisor for later chapters.

Remark 1.2.2. Not all the theta divisors are linearly equivalent. Via considering the divisor $\{(Q, P) : Q \in \Theta_P \subset J, P \in \mathcal{C}\}$ on $J \times \mathcal{C}$, the theta divisors can be checked to be algebraically equivalent. Let $\mathrm{NS}(J)$ denote the *Neron-Severi group* of J, which is the group of divisors on J modulo algebraic equivalence. This implies the equivalence class of any theta divisor is in $H^0(G_K, \mathrm{NS}(J))$. Moreover, for $Q \in J$ corresponding to $\{P_1, P_2\}$, a pair of points on $\mathcal{C}$, $\tau_Q^*\Theta_{P_1} = \Theta_{-P_2}$. Hence, translation by points on J also preserves the algebraic equivalence class of a theta divisor.

Remark 1.2.3. Since Θ corresponds to a Weierstrass point, it can be checked that $2\Theta \sim \Theta^+ + \Theta^-$, where Θ^+ denotes the divisor on J that corresponds to the divisor $\{\infty^+\} \times \mathcal{C} + \mathcal{C} \times \{\infty^+\}$ on $\mathcal{C} \times \mathcal{C}$ and similarly for Θ^-. In particular, this implies that the divisor class of $2n\Theta$ is defined over the base field K, for any positive integer n.

1.2.4 Principal polarization

A *polarized abelian variety* is an abelian variety A equipped with an isogeny $\lambda : A \to A^\vee$, where $A^\vee = \mathrm{Pic}^0(A)$ is the dual abelian variety of A, such that λ

comes from an ample invertible sheaf on $A_{\bar{K}}$. If λ is an isomorphism, then we say (A, λ) is a *principally polarized abelian variety*.

The Jacobian variety (J, λ) is principally polarized via the theta divisor and this polarization is independent of the choice of the theta divisor used:

$$\begin{array}{rccc} \lambda: & J & \longrightarrow & J^\vee \\ & P & \longmapsto & [\tau_P^*\Theta - \Theta]. \end{array}$$

In this thesis, we always assume J is principally polarized via the theta divisor. For simplicity, we will sometimes denote (J, λ) by J.

1.2.5 The Kummer and its desingularization

The *Kummer surface*, denoted by $\mathcal{K}$, is the quotient of J via the involution $[-1] : P \mapsto -P$. The fixed points under the involution are the 16 points of order 2 on J and these map to the 16 nodal singular points of $\mathcal{K}$ (the *nodes*). We let $\mathcal{S}$ denote its desingularization, called the *desingularized Kummer surface*.

1.3 Explicit Embeddings and Defining Equations

This section describes the explicit embeddings of the Jacobian variety J of a genus two curve $\mathcal{C}$ as well as its Kummer surface $\mathcal{K}$ and desingularized Kummer surface $\mathcal{S}$. The details of the material included in this section can be found in [CF96, Chapters 2, 3].

1.3.1 The linear system of $n\Theta$

In this thesis, for a divisor D on a smooth algebraic variety X, we let $\mathcal{L}(D)$ denote $\mathrm{H}^0(X, \mathcal{O}_X(D))$, which is the vector space of global sections of the line bundle associated to D. Sometimes we refer to it as the *Riemann-Roch space* of D. The *linear system* of D, which is the set of effective divisors on X linearly equivalent to D, is denoted by $|D|$.

General theory, as in [Mil08, Theorem 11.1] [Mum70, page 150], shows that the linear system of $n\Theta$ of J has dimension n^2, with $|2\Theta|$ base point free and $|4\Theta|$ very ample. Hence, we know that $|2\Theta|$ induces a morphism defined over K from J to $\mathbb{P}^3$ and $|4\Theta|$ induces an embedding defined over K from J to $\mathbb{P}^{15}$. Note these morphisms are defined over K as explained in Remark 1.2.3. A function g on J is *even* when it is invariant under the involution $[-1] : P \mapsto -P$ and is *odd* when $g \circ [-1] = -g$. Out of the 16 basis elements of $\mathcal{L}(4\Theta)$, 10 of them are even while the other 6 are odd, as shown in the explicit formulae for a set of 16 basis elements given in Section 1.3.3.

1.3.2 Embedding of $\mathcal{K}$ in $\mathbb{P}^3$

From Section 1.3.1, we know that $\dim \mathcal{L}(2\Theta) = 4$ and $|2\Theta|$ induces a morphism from J to $\mathbb{P}^3$. By Remark 1.2.3, we know $2\Theta \sim \Theta^+ + \Theta^-$. Let $\{k_1, k_2, k_3, k_4\}$ denote the basis of $\mathcal{L}(\Theta^+ + \Theta^-)$ with formulae given below. The image of this morphism is precisely the Kummer surface $\mathcal{K}$. We give the explicit formula for this embedding:

Let a genus two curve be given by $\mathcal{C} : y^2 = f(x) = \sum_{j=0}^{6} f_j x^j$ with $f_6 \neq 0$. Denote a generic point on the Jacobian J of $\mathcal{C}$ by $\{(x, y), (u, v)\}$. Then the morphism from J to $\mathbb{P}^3$ is given by

$$k_1 = 1, k_2 = (x + u), k_3 = xu, k_4 = \beta_0,$$

where

$$\beta_0 = \frac{F_0(x, u) - 2yv}{(x - u)^2}$$

with $F_0(x, u) = 2f_0 + f_1(x + u) + 2f_2(xu) + f_3(x + u)(xu) + 2f_4(xu)^2 + f_5(x + u)(xu)^2 + 2f_6(xu)^3$.

In fact, k_1, k_2, k_3 are regular nonzero at $\mathcal{O}_J$ and k_4 has a double pole at $\mathcal{O}_J$. This implies $\mathcal{O}_J$ is mapped to $(0 : 0 : 0 : 1) \in \mathcal{K} \subset \mathbb{P}^3$.

In this thesis, unless stated otherwise, $J \xrightarrow{|2\Theta|} \mathcal{K}$ always denotes the morphism $P \mapsto (k_1(P) : k_2(P) : k_3(P) : k_4(P))$ with k_i given above. We sometimes also let k denote this morphism. It is known that the image of this morphism in $\mathbb{P}^3$ is given by the vanishing of the quartic

$$G(k_1, k_2, k_3, k_4) = G_2 k_4^2 + G_1 k_4 + G_0,$$

where

$$\begin{aligned}
G_2 =& k_2^2 - 4k_1k_3, \\
G_1 =& -2(2f_0k_1^3 + f_1k_1^2k_2 + 2f_2k_1^2k_3 + f_3k_1k_2k_3 + 2f_4k_1k_3^2 + f_5k_2k_3^2 + 2f_6k_3^3), \\
G_0 =& (f_1^2 - 4f_0f_2)k_1^4 - 4f_0f_3k_1^3k_2 - 2f_1f_3k_1^3k_3 - 4f_0f_4k_1^2k_2^2 \\
&+ 4(f_0f_5 - f_1f_4)k_1^2k_2k_3 + (f_3^2 + 2f_1f_5 - 4f_2f_4 - 4f_0f_6)k_1^2k_3^2 - 4f_0f_5k_1k_2^3 \\
&+ 4(2f_0f_6 - f_1f_5)k_1k_2^2k_3 + 4(f_1f_6 - f_2f_5)k_1k_2k_3^2 - 2f_3f_5k_1k_3^3 - 4f_0f_6k_2^4 \\
&- 4f_1f_6k_2^3k_3 - 4f_2f_6k_2^2k_3^2 - 4f_3f_6k_2k_3^3 + (f_5^2 - 4f_4f_6)k_3^4.
\end{aligned}$$

Therefore, the Kummer surface $\mathcal{K} \subset \mathbb{P}^3_{k_i}$ is defined by $G(k_1, k_2, k_3, k_4) = 0$. The following remark is used in the later chapters.

Remark 1.3.1. Suppose $P \in J[2]$. We know $\tau_P^*(2\Theta) \sim 2\Theta$ via the polarization. This implies that the translation by P on J induces a linear isomorphism on $\mathcal{K} \subset \mathbb{P}^3$.

1.3.3 Embedding of J in $\mathbb{P}^{15}$

From Section 1.3.1, we know that $|4\Theta|$ induces an embedding of J in $\mathbb{P}^{15}$. Let $k_{ij} = k_i k_j$, for $1 \leq i \leq j \leq 4$. Since $\mathcal{K}$ is irreducible and defined by a polynomial of degree 4, $k_{11}, k_{12}, ..., k_{44}$ are 10 linearly independent even elements in $\mathcal{L}(2\Theta^+ + 2\Theta^-)$. The six odd basis elements in $\mathcal{L}(2\Theta^+ + 2\Theta^-)$ are given by

$$\begin{aligned} b_i =& \frac{u^{i-1}y - x^{i-1}v}{x-u} \quad (1 \leq i \leq 4), \\ b_5 =& \frac{1}{2f_6}\frac{T(x,u)y - T(u,x)v}{(x-u)^3}, \\ b_6 =& -\frac{1}{4f_6}(f_1b_1 + 2f_2b_2 + 3f_3b_3 + 4f_4b_4 + 4f_5b_5 - f_5k_3b_3 + f_5k_2b_4 - 2f_6k_3b_4 \\ & + 2f_6k_2b_5), \end{aligned}$$

with

$$\begin{aligned} T(r,s) =& 4f_0 + f_1(r+3s) + 2f_2s(r+s) + f_3s^2(3r+s) + 4f_4rs^3 + f_5s^4(5r-s) \\ & + 2f_6rs^4(r+s). \end{aligned}$$

In this thesis, unless stated otherwise, we always use $k_{11}, k_{12}, ..., k_{44}, b_1, ..., b_6$, as basis of $\mathcal{L}(2\Theta^+ + 2\Theta^-)$, to embed J in $\mathbb{P}^{15}$. The following theorem and remarks give more details on this embedding.

Theorem 1.3.2. *([Fly90, Therorem 1.2], [Fly93, Therorem 1.2]) Let J be the Jacobian variety of the genus two curve $\mathcal{C}$ defined by $y^2 = f_6x^6 + ... + f_1x + f_0$. The 72 quadratic forms over $\mathbb{Z}[f_0, ..., f_6]$ given in [Fly90, Appendix A] are a set of defining equations for the projective variety given by the embedding of J in $\mathbb{P}^{15}$ induced by the basis of $\mathcal{L}(2\Theta^+ + 2\Theta^-)$ with explicit formulae given in [Fly90, Definition 1.1] or [Fly93, Definition 1.1]. The change of basis between this set of basis of $\mathcal{L}(2\Theta^+ + 2\Theta^-)$ and $k_{11}, k_{12}, ..., k_{44}, b_1, ..., b_6$ is given in [FTvL12, Section 3].*

Remark 1.3.3. Suppose we embed J via $k_{11}, k_{12}, ..., k_{44}, b_1, ..., b_6$. By [Fly90, Appendix A], as described in [FTvL12, Section 3], the 72 defining equations consist of 30 odd quadratics where each monomial is a product of an even coordinate and an odd coordinate, 21 quadratics involving only the even coordinates and 21 quadratics in the form of $b_ib_j = Q_{ij}$, where Q_{ij} is a quadratic in terms of the 10 even coordinates.

Remark 1.3.4. Suppose $P \in J[2]$. Via the same argument as in Remark 1.3.1, we get τ_P is a linear isomorphism on $J \subset \mathbb{P}^{15}$. Moreover, we know $\tau_P^* k_{ij}$ is even

and $\tau_P^*(b_i)$ is odd. This implies that the matrix representation of the linear isomorphism τ_P on $J \subset \mathbb{P}^{15}$ is block diagonal with a block of size 10 corresponding the even coordinates and a block of size 6 corresponding to the odd coordinates.

We quote the following nice results that are needed in the later chapters of the thesis.

Theorem 1.3.5. [Fly93, Theorem 3.2] *Let J be the Jacobian variety of the genus two curve $\mathcal{C}$ defined by $y^2 = f_6x^6 + ... + f_1x + f_0$. Let $a, b \in J \subset \mathbb{P}^{15}$ with coordinates $k_{11}, k_{12}, ..., k_{44}, b_1, ..., b_6$. Then there exists a 4×4 matrix of bilinear forms $\phi_{ij}(a, b)$ defined over $\mathbb{Z}[f_0, ..., f_6]$ which is projectively equal to the matrix $k_i(a-b)k_j(a+b)$. The explicit formula for ϕ_{ij} is given in* [Fly93, Appendix B] *with the relevant change of basis given in* [FTvL12, Section 3].

Remark 1.3.6. The bilinear forms ϕ_{ij} defined in Theorem 1.3.5 have the following properties as given in [Fly93, Remark 3.3].

(i) $\phi_{ij}(a, b) = \phi_{ij}(-a, -b)$. In particular, each bilinear form contains only even·even terms and odd·odd terms.

(ii) $\phi_{ij}(a, b) = \phi_{ij}(b, a)$.

(iii) $\phi_{ji}(a, b) = \phi_{ij}(a, -b)$. This implies that ϕ_{ji} may be induced from ϕ_{ij} by leaving the even·even terms unchanged and negating the odd·odd terms. Therefore $\phi_{ij} + \phi_{ji}$ only contains even·even terms.

We deduce the following corollary from Theorem 1.3.5 and Remark 1.3.6 above.

Corollary 1.3.7. *(*[Fly93, Lemma 2.2], [CF96, Theorem 3.4.1]*) Let J be the Jacobian variety of the genus two curve $\mathcal{C}$ defined by $y^2 = f_6x^6 + ... + f_1x + f_0$. Let $a, b \in J \subset \mathbb{P}^{15}$ with coordinates $k_{11}, k_{12}, ..., k_{44}, b_1, ..., b_6$. Let $k(a) = (k_1(a), ..., k_4(a))$ and $k(b) = (k_1(b), ..., k_4(b))$. Then, there exist biquadratic forms ψ_{ij} defined over $\mathbb{Z}[f_0, ..., f_6]$ such that the 4×4 matrix $\psi_{ij}(k(a), k(b))$ is projectively equal to $k_i(a+b)k_j(a-b) + k_i(a-b)k_j(a+b)$. In particular, each ψ_{ij} is symmetric and we have an explicit formula for ψ_{ij}.*

Proof. By Theorem 1.3.5, we have the 4×4 matrix of bilinear forms $\phi_{ij}(a, b)$ defined over $\mathbb{Z}[f_0, ..., f_6]$ which is projectively equal to the matrix $k_i(a-b)k_j(a+b)$. By Remark 1.3.6(ii) and (iii), $\psi_{ij} = \phi_{ij} + \phi_{ji}$ are symmetric biquadratic forms satisfying the lemma.

□

1.3.4 Embedding of $\mathcal{S}$ in $\mathbb{P}^5$

In this section, we describe the explicit embedding of a nonsingular surface $\mathcal{S}$ in $\mathbb{P}^5$, that is canonically birationally equivalent to $\mathcal{K}$ and is a minimal desingularization of it. More details can be found in [CF96, Chapter 16] and [FTvL12, Section 4].

The surface $\mathcal{S}$

Recall that our genus two curve $\mathcal{C}$ is defined by $y^2 = f(x) = f_6x^6 + ... + f_0$, with $f_i \in K$ and $f_6 \neq 0$. Let $(p_0 : p_1 : ... : p_5)$ be a point in $\mathbb{P}^5$, and define $P(x) = \sum_{j=0}^{5} p_j x^j$. We know $P(x)^2$ is congruent to a polynomial of degree at most 5:

$$f_6^5 P(x)^2 \equiv \sum_{j=0}^{5} c_j x^j \mod f(x)$$

where c_j are quadratic forms in $\{p_0, ..., p_5\}$ with coefficients in $\mathbb{Z}[f_0, ..., f_6]$.

The surface $\mathcal{S}$ embedded in $\mathbb{P}^5$ is defined to be the locus of $(p_0 : ... : p_5)$ for which $P(x)^2$ is congruent to a quadratic in x modulo $f(x)$. Hence, it is defined by the intersection of 3 quadric surfaces:

$$\mathcal{S} : c_5 = c_4 = c_3 = 0.$$

Relationship with J and $\mathcal{K}$

We follow the discussion in [CF96, Chapter 16, Section 3]. Suppose a general point $P \in J$ is represented by $\{(x_1, y_1), (x_2, y_2)\}$. There is a unique $M(x)$ of degree 3 such that $y = M(x)$ meets $\mathcal{C}$ twice at $(x_1, y_1), (x_2, y_2)$. Then $M(x)^2 - f(x) = (x - x_1)^2(x - x_2)^2H(x)$ for some quadratic $H(x)$. Note that $H = 0, y = -M(x)$ gives the point $2P \in J$ via the group law on J described in Section 1.2.2. There is a unique polynomial $Q(x) = \sum_{j=0}^{5} q_j x^j$ of degree at most 5 such that

$$(x - x_1)(x - x_2)Q \equiv M(x) \mod f(x),$$

which implies that $Q(x)^2 \equiv H(x) \mod f(x)$. We have $(q_0 : ... : q_5)$ is the corresponding element to P on $\mathcal{S}$.

Furthermore, the coefficients of $Q(x)$ are symmetric in $(x_1, y_1), (x_2, y_2)$ and hence are in the function field of J. It can be checked that they are in fact odd functions. This implies that multiplying $Q(x)$ by any odd function on J, for example $(y_1 - y_2)/(x_1 - x_2)$, will make the coefficients even functions and so in the function field of $\mathcal{K}$. This gives a rational map $\mathcal{K} \to \mathcal{S}$.

It can also be shown that the embedding of $\mathcal{S}$ in $\mathbb{P}^5$ is isomorphic to the projection of $J \subset \mathbb{P}^{15} \to \mathbb{P}^5$ onto the 6 odd coordinates:

$$P \mapsto (b_1(P) : ... : b_6(P)).$$

More explicitly, define

$$g_i = \sum_{j=i}^{6} f_j x^{j-i}, \text{ for } i \in 1, ..., 6,$$

and we quote the following proposition.

Proposition 1.3.8. [FTvL12, Proposition 4.11] *Let $\mathcal{C}$ be a genus two curve defined by $y^2 = f(x)$, with $f(x)$ a degree 6 polynomial and $L = K[x]/(f)$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on $\mathcal{C}$ that are not Weierstrass points and $x_1 \neq x_2$. Embed the Jacobian variety J in $\mathbb{P}^{15}$ with coordinates $k_{11}, k_{12}, ..., k_{44}, b_1, ..., b_6$ as in Section 1.3.3 and denote the point $\{P_1, P_2\} \in J$ by P. Define $M(x)$ to be the unique cubic polynomial such that the curve $y = M(x)$ meets $\mathcal{C}$ twice at P_1 and P_2. Setting $Q(x)$ to be the polynomial of degree at most 5, satisfying*

$$Q(x) = M(x)(x - x_1)^{-1}(x - x_2)^{-1} \in \bar{L},$$

we have that $Q(x) = \sum_{i=1}^{6} b_i(P) g_i(x)$ up to scalar multiple.

Note: the coefficients of $Q(x)$ give the point in $\mathcal{S} \subset \mathbb{P}^5$ that corresponds to $P \in J$.

It can be seen from the above proposition, that the map $J \subset \mathbb{P}^{15} \to \mathbb{P}^5$ given by the odd coordinates gives a rational map from J to $\mathcal{S}$.

Remark 1.3.9. As explained in Remark 1.3.3, all quadratic polynomials in the b_i can be expressed as quadratics in the k_{ij}, or as quartics in the k_i. This induces a rational map from $\mathcal{K}$ to $\mathcal{S}$ that is the inverse of the blow-up morphism $\mathcal{S} \to \mathcal{K}$. This morphism can be described, as in [FTvL12, Remark 3.8], explicitly as

$$(b_1 : ... : b_6) \mapsto (k_1 : k_2 : k_3 : k_4)$$
$$= (b_1b_3 - b_2^2 : b_1b_4 - b_2b_3 : b_2b_4 - b_3^2 : f_0b_1^2 + f_1b_1b_2 + f_2b_2^2 + f_3b_2b_3 + f_4b_3^2 + f_5b_3b_4 + f_6b_4^2).$$

1.4 Galois Cohomology and the Brauer Group

In this section, we give some basic notations and background theory on Galois cohomology and the Brauer group. Most material comes form [Ser79, Parts Three and Four].

1.4.1 Galois cohomology for abelian groups

For any group G and any G-module A, we denote the group of n^{th} cochains, cocycles and coboundaries by $C^n(G,A)$, $Z^n(G,A)$ and $B^n(G,A)$, respectively. We denote the n^{th} cohomology by $H^n(G,A) := Z^n(G,A)/B^n(G,A)$. For simplicity, we denote the connecting homomorphism $C^i(G,A) \to C^{i+1}(G,A)$ by d for all $i \in \mathbb{N}$. It most cases, G will be a Galois group in this thesis.

We have explicit formulae for the connecting homomorphisms. In particular, $d : C^0(G,A) \to C^1(G,A)$ is explicitly given by $d(a)(g) = ga - a$ for $g \in G, a \in A$ representing an element in $C^0(G,A)$ and $d : C^1(G,A) \to C^2(G,A)$ is explicitly defined by:

$$d(\phi)(g_1,g_2) = g_1\phi(g_2) - \phi(g_1g_2) + \phi(g_1),$$

for $g_1, g_2 \in G, \phi \in C^1(G,A)$.

Notation 1.4.1. Let A, B be G_K-modules. For a surjective G_K-homomorphism $f : A \to B$, we have the short exact sequence $0 \to A[f] \to A \xrightarrow{f} B \to 0$ of G_K-modules. We let $\delta_{i,f} : H^i(G_K, B) \to H^{i+1}(G_K, A[f])$ denote the connecting map in the long exact sequence induced by the short exact sequence. In the case where K is a global field, we also let $\delta_{i,f}$ denote the connecting map $H^i(G_{K_v}, B) \to H^{i+1}(G_{K_v}, A[f])$ for each place v of K for simplicity. Sometimes, we abbreviate $\delta_{i,f}$ to δ_i or even to δ, when the context is clear.

Definition 1.4.2. Let $\phi : A \to B$ be an isogeny between two principally polarized abelian varieties defined over a number field K. Define the *ϕ-Selmer group* of A, denoted by $\mathrm{Sel}^\phi(A)$, to be $\ker\left(H^1(G_K, A[\phi]) \to \prod_v H^1(G_{K_v}, A)\right)$, and the *Tate-Shafarevich group* of A, denoted by $Ш(A)$, to be $\ker\left(H^1(G_K, A) \to \prod_v H^1(G_{K_v}, A)\right)$.

1.4.2 Galois cohomology for non-abelian groups

In this section, we discuss the Galois cohomology of non-abelian groups. Let G be a group and A a group on which G acts on the left. In this case, $H^0(G,A)$ is still defined as the group of elements in A fixed by G as in the abelian case. We define *cocycles* to be maps $s \mapsto a_s$ of G into A such that $a_{st} = a_s \cdot s(a_t)$, writing A multiplicatively. Similarly, we say a_s, b_s are *cohomologous* if there exists $a \in A$ such that $b_s = a^{-1} \cdot a_s \cdot s(a)$ for all $s \in G$, which gives an equivalence relation for the set of cocycles. Provided with the structure of a distinguished element equal to the class of the unit cocycle $a_s = 1$, we can still define the quotient set $H^1(G,A)$. This coincides with the definition in the abelian case except $H^1(G,A)$ is now a pointed set instead of a group. This is discussed in full detail in [Ser79, Chapter VII Appendix].

Moreover we quote the following two propositions on the induced long exact sequences from the short exact sequences, that we will use later in this

thesis. In particular, it can be checked that the connecting maps δ_1, δ_2 in the propositions below are well-defined via the similar definition as the abelian case.

Proposition 1.4.3. [Ser79, Chapter VII Appendix, Proposition 1] *Let* $1 \to A \xrightarrow{i} B \xrightarrow{p} C \to 1$ *be an exact sequence of non-abelian* G*-modules. Then the sequence of pointed sets below is exact:*

$$1 \to H^0(G, A) \to H^0(G, B) \to H^0(G, C) \xrightarrow{\delta_1} H^1(G, A) \to H^1(G, B) \to H^1(G, C).$$

Proposition 1.4.4. [Ser79, Chapter VII Appendix, Proposition 2] *In addition to the hypothesis of 1.4.3, assume that* A *is in the center of* B*. Then the sequence of pointed sets below is exact:*

$$\begin{aligned} 1 \to H^0(G, A) \to H^0(G, B) \to & H^0(G, C) \xrightarrow{\delta_1} H^1(G, A) \\ & \to H^1(G, B) \to H^1(G, C) \xrightarrow{\delta_2} H^2(G, A). \end{aligned}$$

1.4.3 Brauer Group

In this section, we discuss the relationship between the Galois cohomology and the Brauer group. We state some definitions and key properties here.

The *Brauer group* of a field K, denoted by $\mathrm{Br}(K)$, is the group of equivalence classes of central simple K-algebras. Recall that a central simple K-algebra A is a finite-dimensional K-algebra which is *central* meaning the centre of A is K, and *simple* meaning that it has no nontrivial two-sided ideals. The set of such algebras is closed under taking the tensor product. Two central simple algebras A_1 and A_2 are called equivalent if $A_1 \otimes_K \mathrm{Mat}_n(K)$ is isomorphic to $A_2 \otimes_K \mathrm{Mat}_m(K)$ for some positive integers n and m. The group law in $\mathrm{Br}(K)$ is induced by the tensor product.

Remark 1.4.5. We observe that matrix algebras are equivalent and in fact they give the identity element in $\mathrm{Br}(K)$. To a central simple algebra A, we can associate its opposite algebra A^{op}, that is, A with the reversed order of multiplication. One checks that $A \otimes_K A^{op}$ is isomorphic to a matrix algebra and this gives inverses of elements in $\mathrm{Br}(K)$. Thus the set of equivalence classes of central simple algebras is indeed a group under the tensor product and we will write $+$ to denote the group operation in this thesis.

Proposition 1.4.6. [Ser79, Chapter X Section 5 Proposition 7] *Let K be a field and A a finite-dimensional K-algebra. The following are equivalent.*

(i) *A has no non-trivial two-sided inverse and its center is K.*

(ii) *A is isomorphic to a matrix algebra over $\bar{K}$.*

(iii) *A is isomorphic to a matrix algebra over some finite Galois extension of K.*

(iv) *A is isomorphic to a matrix algebra over a division algebra with center K.*

By Proposition 1.4.6, we know there are three other equivalent definitions for central simple algebras. In particular, the definition (iv) above is a consequence of Wedderburn's Theorem, which we state next.

Theorem 1.4.7 (Wedderburn)**.** *Let A be a finite dimensional central simple K-algebra. Then there is some finite-dimensional (as a K-vector space) division algebra $D \supset K$ and some $n > 0$ such that $A \cong M_n(D)$, and D, n are unique.*

Remark 1.4.8. By Wedderburn's Theorem, another way to define the equivalence relationship of central simple algebras in the definition of Brauer group is the following. We say two central simple algebras are equivalent if their division algebras associated by Proposition 1.4.6(iv) are K-isomorphic. Moreover, when two central simple algebras have the same dimension, equivalence reduces to being K-isomorphic. This is discussed in [Ser79, Chapter X Section 5].

Example 1.4.9. Quaternion Algebra: Let $a, b \in K^*$. The *quaternion algebra* (a, b) is the unique K-algebra of dimension 4 with K-basis $1, i, j, k$ such that

- $i^2 = a$,
- $j^2 = b$,
- $ij = -ji = k$.

Note that (a, b) only depends on a, b up to squares in K^*. Also, quaternion algebras represent elements of $\mathrm{Br}[2]$ as for any quaternion algebra A, $A \cong A^{op}$.

Remark 1.4.10. By Remark 1.4.8, we know two quaternion algebras representing the same element in $\mathrm{Br}[2]$ are isomorphic. We will sometimes denote the class of the quaternion algebra (a, b) by (a, b), which is an element in $\mathrm{Br}[2]$.

From the results in [Ser79, Chapter XIV, Section 2 Proposition 4] and [GS06, Corollary 2.5.5(1), Proposition 4.7.3], we have the following proposition which we will use later in the thesis.

Proposition 1.4.11. *The followings are some properties of quaternion algebras:*

(i) $(ab, c) = (a, c) + (b, c)$

(ii) $(a, bc) = (a, b) + (a, c)$

(iii) $(a, b) = 0$ *if and only if* b *is a norm in the extension* $K(\sqrt{a})/K$.

Remark 1.4.12. From Proposition 1.4.11(iii), we know that a quaternion algebra (a, b) is trivial, which means that it is isomorphic to $\mathrm{Mat}_2(K)$, if and only if $ax^2 + by^2 = z^2$ is solvable over K.

One important and well-known result on the Brauer group is the following isomorphism. The proof is nontrivial and we refer to [Ser79, Chapter X Section 5 Proposition 9] and [GS06, Theorem 4.4.3] for a proof.

Proposition 1.4.13. *We have the following isomorphism*

$$Br(K) \cong H^2(G_K, \bar{K}^*).$$

Remark 1.4.14. In this remark, we give a description of the above isomorphism following the proof. Let $\mathrm{CSA}(n)$ denote the set of isomorphism classes of central simple K-algebras that are isomorphic to $\mathrm{Mat}_n(K)$ over $\bar{K}$. There is a canonical bijection $\mathrm{CSA}(n) \xrightarrow{f_n} H^1(G_K, \mathrm{PGL}_n)$, sending A to $(\sigma \mapsto M_\sigma \in \mathrm{PGL}_n)$ where $\phi : A \otimes \bar{K} \cong \mathrm{Mat}_n(\bar{K})$ and $\phi(\phi^{-1})^\sigma \in \mathrm{Aut}(\mathrm{Mat}_n)$ is conjugation by M_σ via the Noether Skolem Theorem. Now for any central simple algebra A, it is in $\mathrm{CSA}(n)$ for some n. The image of the class of A under the isomorphism in Proposition 1.4.13 is precisely the image of $f_n(A)$ in $H^2(G_K, \bar{K}^*)$ via the injective connecting map $H^1(G_K, \mathrm{PGL}_n) \to H^2(G_K, \bar{K}^*)$ induced by the short exact sequence: $1 \to \bar{K}^* \to \mathrm{GL}_n \to \mathrm{PGL}_n \to 1$.

Corollary 1.4.15. *We have the following isomorphism*

$$Br(K)[n] \cong H^2(G_K, \mu_n).$$

Proof. The result follows from Proposition 1.4.13 and Hilbert's Theorem 90 via the short exact sequence: $1 \to \mu_n \to \bar{K}^* \xrightarrow{x \mapsto x^n} \bar{K}^* \to 1$.

□

Remark 1.4.16. Consider the natural pairing $\phi : \mu_2 \times \mu_2 \to \mu_2$ sending $((-1)^a, (-1)^b)$ to $(-1)^{ab}$. This gives a pairing

$$\begin{array}{ccc} H^1(G_K, \mu_2) \times H^1(G_K, \mu_2) & \longrightarrow & H^2(G_K, \mu_2) \cong \mathrm{Br}(K)[2] \\ ([\sigma \mapsto a_\sigma], [\tau \mapsto b_\tau]) & \longmapsto & [(\sigma, \tau) \mapsto \phi(a_\sigma, b_\tau)] \end{array}.$$

By Hilbert's Theorem 90, we can identify $H^1(G_K, \mu_2)$ with $K^*/(K^*)^2$. Under this identification, the image of $(a, b) \in K^*/(K^*)^2 \times K^*/(K^*)^2$ is precisely the equivalence class of the quaternion algebra (a, b) by [Ser79, Chapter XIV, Section 2, Proposition 5] and [GS06, Corollary 2.5.5(1), Proposition 4.7.3].

1.4.4 Invariant Map and Hilbert Symbol

In this section, we state some key properties of the invariant map of the Brauer group and discuss its relationship with the Hilbert Symbol for quaternion algebras.

Invariant map

- **Local:** Let K be a non-archimedean local field of characteristic 0. Local class field theory provides a local invariant map, $\mathrm{inv} : \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}$, which is an isomorphism. In particular, $\mathrm{inv} : \mathrm{Br}(K)[n] \cong \mathbb{Z}/n\mathbb{Z}$. Note, in the case $n = 2$, we sometimes replace $(\mathbb{Z}/2\mathbb{Z}, +)$ with $(\mu_2, \times)$.
- **Global:** Let K be a number field. We have the following exact sequence:

$$0 \to \mathrm{Br}(K) \to \bigoplus_v \mathrm{Br}(K_v) \xrightarrow{\sum_v \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \to 0.$$

Hilbert symbol

In the case where K is a local field or $K = \mathbb{R}$, the *Hilbert symbol* or the *norm residue symbol*, denoted by $(\ ,\ )_H : K^* \times K^* \to \{1, -1\}$, is explicitly defined as follows:

$(a, b)_H = 1$ if and only if $z^2 = ax^2 + by^2$ has a nontrivial solution over K^3.

From this definition, we can see that $(a, b)_H$ only depends on a, b up to squares in K^*. By the results in [Ser79, Chapter XIV, Section 2 Proposition 7 and Remark(3) after Proposition 4] and the fact that the local invariant map is injective, we have the following proposition which is used in the later chapters

of the thesis.

Proposition 1.4.17. *The following are some properties of the Hilbert symbol.*

(i) $(aa', b)_H = (a, b)_H \cdot (a', b)_H$

(ii) $(a, bb')_H = (a, b)_H \cdot (a, b')_H$

(iii) $(a, b)_H = 1$ *if and only if* b *is a norm in the extension of* $K(\sqrt{a})/K$.

The Hilbert symbol has an explicit formula and it has been implemented in MAGMA. Here, we describe the formula in the case where the local field $K = \mathbb{Q}_p$, as in [Ser79, Chapter XIV, Section 4].

For $K = \mathbb{Q}_p$ with $p \neq 2$, the formula for $(a, b)_H$ is the following:

Let $a = p^\alpha a', b = p^\beta b'$, where a', b' are units in $\mathbb{Z}_p$. Define $c := (-1)^{\alpha\beta} \frac{a'^\beta}{b'^\alpha}$. Then

$$(a, b)_H = (-1)^{\frac{p-1}{2}\alpha\beta} \left(\frac{b'}{p}\right)^\alpha \left(\frac{a'}{p}\right)^\beta,$$

where the Legendre symbol $\left(\frac{x}{p}\right) = x^{(p-1)/2}$ for any $x \in \mathbb{F}_p^*$. Note that the Legendre symbol naturally extends to $\mathbb{Z}_p^*$.

For $K = \mathbb{Q}_2$, we have $(2, 2)_H = 1$ and the following formulae:

$$(2, u)_H = (-1)^{w(u)} \text{ if } u \text{ is in } \mathbb{Z}_2^*,$$
$$(u, v)_H = (-1)^{\epsilon(u)\epsilon(v)} \text{ if } u, v \text{ both in } \mathbb{Z}_2^*,$$

where $w(x)$ is the coset mod 2 of $(x^2 - 1)/8$ for any $x \in \mathbb{Z}_2^*$ and $\epsilon(x)$ is the coset mod 2 of $(x - 1)/2$ for any $x \in \mathbb{Z}_2^*$.

One useful lemma on the Hilbert symbol is the following.

Lemma 1.4.18. *Let* K *be a local field. If* $a, b \in K^*$ *both have valuation 0 and* K *has odd residue characteristic, then*

$$(a, b)_H = 1.$$

Proof. By definition we know $(a, b)_H = 1$ if and only if $z^2 = ax^2 + by^2$ has a nontrivial solution in K^3. Since a, b have valuation 0, $z^2 = ax^2 + by^2$ defines a smooth conic and the reduction of this conic over the residue field $\mathbb{F}_q$, where q is some power of some prime $p \neq 2$, is a smooth curve of genus zero. Hence, by the Hasse-Weil bound, the number of $\mathbb{F}_q$-points on the reduction of the conic is precisely equal to $q + 1$. By Hensel's Lemma [HS00, Exercise C.9(c)], we can

always find a nontrivial solution of $z^2 = ax^2 + by^2$ as required.

□

By the definition of the Hilbert symbol, the injectivity of the local invariant map and Remark 1.4.12, we also have the following lemma relating the Hilbert symbol and the invariant map in the case of a quaternion algebra.

Lemma 1.4.19. *Consider a quaternion algebra (a, b) over a local field K. Let (a, b) denote its equivalence class in $Br(K)$,*

$$inv\big((a, b)\big) = (a, b)_H.$$

1.5 Principal Homogeneous Spaces and n-Coverings

In this section, we state some definitions concerning the twists of the Jacobian variety J as well as some useful propositions needed later in the thesis. Similar results in the elliptic curves are in [CFO+08]. Note, unless stated otherwise, a twist in this thesis means $\bar{K}/K$ twist, that is an isomorphic variety defined over K with the isomorphism defined over $\bar{K}$. We first state the following well-known proposition for twists.

Proposition 1.5.1. [Ser97, Chapter III, Section 1, Proposition 5] *Let X be a quasi-projective variety defined over K. There is a natural bijection between the set of isomorphism classes of the twists of X and $H^1(G_K, Aut(X_{\bar{K}}))$ that sends a twist A to the class of cocycle $\sigma \mapsto \phi \circ \sigma(\phi^{-1})$, for a fixed choice of isomorphism $\phi : A_{\bar{K}} \to X_{\bar{K}}$.*

1.5.1 Principal homogeneous space

A *principal homogeneous space or a torsor* for an abelian variety A defined over a field K is a variety V together with a morphism $\mu : A \times V \to V$, both defined over K, that induces a simply transitive action of $A(\bar{K})$ on $V(\bar{K})$.

We say (V_1, μ_1) and (V_2, μ_2) are isomorphic over a field extension K_1 of K if there is an isomorphism $\phi : V_1 \to V_2$ defined over K_1 such that the following diagram commutes.

$$\begin{array}{ccccc} A & \times & V_1 & \xrightarrow{\mu_1} & V_1 \\ \downarrow{=} & & \downarrow{\phi} & & \downarrow{\phi} \\ A & \times & V_2 & \xrightarrow{\mu_2} & V_2 \end{array}$$

We observe that $(A, +)$ is a trivial principal homogeneous space for A and we have the following lemma.

Lemma 1.5.2. *Let A be an abelian variety defined over K. The only isomorphism $\phi : A \to A$ as the trivial torsor is translation by some $P \in A$.*

Proof. Consider the following commutative diagram.

$$\begin{array}{ccccc} A & \times & A & \xrightarrow{+} & A \\ \downarrow{=} & & \downarrow{\phi} & & \downarrow{\phi} \\ A & \times & A & \xrightarrow{+} & A \end{array}$$

We have $Q+\phi(\mathrm{id}) = \phi(Q)$, for any $Q \in A$. Here, id denotes the identity element in A

□

For simplicity, we sometimes denote (V, μ) by V and we have the following proposition whose proof we omit.

Proposition 1.5.3. [LT58, Proposition 4] *Let A be an abelian variety defined over K. There is a canonical bijection between $H^1(G_K, A)$ and the set of isomorphism classes of principal homogeneous spaces for A over K.*

Remark 1.5.4.

(i) From the proof of the above proposition, we know that for a principal homogeneous space V of A with a morphism $\mu : A \times V \to V$ and a point $P \in V(\bar{K})$, the map $Q \mapsto \mu(Q, P)$ for all $Q \in A$ gives an isomorphism of principal homogeneous spaces defined over $K(P)$. Denote the inverse of this isomorphism by $\phi : V \to A$, then we have $\phi \cdot (\phi^{-1})^\sigma$ is a translation by a point $P_\sigma \in A$ and $(\sigma \mapsto P_\sigma)$ gives the corresponding element in $H^1(G_K, A)$. Note that different choices of the point P give the same cocycle up to coboundaries.

(ii) Let V be a principal homogeneous space of A with an isomorphism $\phi : V \to A$ such that $\phi(\phi^{-1})^\sigma$ is translation by $\epsilon_\sigma \in J$ and $(\sigma \mapsto \epsilon_\sigma)$ is a cocycle representing ϵ. Then for $P \in J$, $\tau_P \circ \phi : V \to A$ is an isomorphism such that it induces the cocycle representation of ϵ that differs from $(\sigma \mapsto \epsilon_\sigma)$ by a coboundary of $(\sigma \mapsto \sigma(P) - P)$.

Remark 1.5.5. With this geometric interpretation, $H^1(G_K, A)$ is called the *Weil-Chatelet group*. By [LT58, Proposition 5], we know the Weil-Chatelet group is a torsion group, i.e. every element of it has finite order.

Corollary 1.5.6. *Let A be an abelian variety defined over K. V is a trivial principal homogeneous space if and only if V has a K-rational point.*

Proof. If V is a trivial principal homogeneous space, that is, there exists an isomorphism $A \cong V$ over K, then the image of the identity element of A in V is defined over K. On the other hand, if there exists $P \in V(K)$, then by Proposition 1.5.3 and Remark 1.5.4 (i), we know that the map $Q \mapsto \mu(Q, P)$ for all $Q \in A$ gives an isomorphism of principal homogeneous spaces $A \cong V$ defined over $K(P) = K$, where $\mu : A \times V \to V$ is the action associated to V.

□

1.5.2 n-coverings

For an integer $n \geq 2$, an *n-covering* of an abelian variety A is a variety X defined over K together with a morphism $\pi : X \to A$ defined over K, such that there exists an isomorphism $\phi : X_{\bar{K}} \to A_{\bar{K}}$ with $\pi = [n] \circ \phi$, shown in the commutative diagram below. An isomorphism $(X_1, \pi_1) \to (X_2, \pi_2)$ between two n-coverings is an isomorphism $h : X_1 \to X_2$ defined over K with $\pi_1 = \pi_2 \circ h$.

$$\begin{array}{ccc} X & & \\ \downarrow{\scriptstyle \phi} & \searrow^{\pi} & \\ A & \xrightarrow{\cdot n} & A \end{array}$$

We sometimes denote (X, π) by X when the context is clear.

In the proposition below, we show that an n-covering of an abelian variety A is a principal homogeneous space of A.

Proposition 1.5.7. *Let A be an abelian variety defined over K and (X, π) be an n-covering of A for some n. X is a principal homogeneous space of A with the simply transitive action $\mu : (P, Q) \mapsto \phi^{-1}(P + \phi(Q))$ for any $P \in A, Q \in X$ and isomorphism $\phi : X \to A$ such that $[n] \circ \phi = \pi$.*

Proof. Since (X, π) is an n-covering of A, there exists an isomorphism $\phi : X \to A$ defined over $\bar{K}$ such that $[n] \circ \phi = \pi$. Since ϕ is an isomorphism, we know $\mu : (P, Q) \mapsto \phi^{-1}(P + \phi(Q))$ for any $P \in A, Q \in X$ induces a simply transitive action of $A(\bar{K})$ on $X(\bar{K})$.

It suffices to show that μ is defined over K. Since $\pi = [n] \circ \phi$ is defined over K, we know $[n] = [n] \circ \phi(\phi^{-1})^{\sigma}$ for all $\sigma \in G_K$. So fix $\sigma \in G_K$, we have a morphism $\alpha_\sigma : A \to A[n]$ that sends P to $\phi(\phi^{-1})^{\sigma}(P) - P$. Since α_σ is continuous and $A[n]$ is a discrete set, we know α_σ is locally constant. The connectedness of

A implies that α_σ is indeed a constant morphism. Hence, there exists $P_\sigma \in A[n]$ such that $\phi(\phi^{-1})^\sigma(P) = P + P_\sigma$. Now to show $\mu^\sigma(P,Q) = \mu(P,Q)$, it suffices to show $P + \phi(Q) = \phi(\phi^{-1})^\sigma(P + \phi^\sigma(Q))$. Since the right hand side is equal to $\phi(\phi^{-1})^\sigma(P + \phi^\sigma\phi^{-1}\phi(Q))$ and $\phi(\phi^{-1})^\sigma = \tau_{P_\sigma}$, we are done.

□

The following lemma and proposition show that the isomorphism classes of n-coverings of A are parameterized by $H^1(G_K, A[n])$. The case when $n = 2$ $A = J$ is proved in [FTvL12, Lemmas 2.13, 2.14] and the result in the elliptic curve case is in [CFO+08, Proposition 1.14]. For completeness, we include the proof in the general case following the proof in [FTvL12] .

Lemma 1.5.8. *Let (X, π) be an n-covering of an abelian variety A defined over K. Suppose there are two isomorphisms defined over $\bar{K}$, $\phi, \phi' : X \to A$, satisfying $[n] \circ \phi = [n] \circ \phi' = \pi$. Then there exists a unique point $P \in A[n]$ such that $\phi' = \tau_P \circ \phi$.*

Proof. Consider the map $\tau : Q \mapsto \phi'(Q) - \phi(Q)$. We have $n(\phi'(Q) - \phi(Q)) = \pi(Q) - \pi(Q) = 0$, which implies that $\tau(Q) \in A[n]$ for all $Q \in X$. Since $A[n]$ is discrete and τ is continuous, we get τ is locally constant. The connectedness of A implies that τ is constant, as required.

□

By the lemma above, we make the following remark.

Remark 1.5.9. Fix (X, π) an n-covering of an abelian variety A of dimension d. Since $|A[n]| = n^{2d}$ by Lemma 1.7.2, Lemma 1.5.8 shows there are precisely n^{2d} different choices for the isomorphism $\phi : X \to A$ such that $[n] \circ \phi = \pi$.

Proposition 1.5.10. *Let (X, π) be an n-covering of an abelian variety A defined over K and choose an isomorphism ϕ such that $\pi = [n] \circ \phi$. Then for each $\sigma \in G_K$, there is a unique point $P \in A[n](\bar{K})$ satisfying $\phi \circ \sigma(\phi^{-1}) = \tau_P$. The map $\sigma \mapsto P$ induces a well-defined cocycle class in $H^1(G_K, A[n])$ that does not depend on the choice of ϕ. This yields a bijection between the set of isomorphism classes of n-coverings of A and the set $H^1(G_K, A[n])$.*

Proof. For $\sigma \in G_K$, $\pi = [n] \circ \phi$ implies $\pi = [n] \circ \sigma(\phi)$. Let $\phi' = \sigma(\phi)$ for some $\sigma \in G_K$ and apply Lemma 1.5.8, we get the unique existence of the point P. It can be checked that for any choice of ϕ, the induced map $\sigma \mapsto P$ is a cocycle. By Lemma 1.5.8, we know different choices of ϕ give rise to the same cocycle class in $H^1(G_K, A[n])$. We also check that two isomorphic n-coverings indeed correspond to the same element in $H^1(G_K, A[n])$. Suppose the n-coverings (X_1, π_1) and (X_2, π_2) both correspond to the same element in $H^1(G_K, A[n])$ and we fix

$\phi_1 : X_1 \to A, \phi_2 : X_2 \to A$ such that $[n] \circ \phi_1 = \pi_1, [n] \circ \phi_2 = \pi_2$. Then by composing ϕ_2 with τ_P for a suitable $P \in J[n]$, we may assume $\phi_1(\phi_1^{-1})^\sigma = \phi_2(\phi_2^{-1})^\sigma$ which implies X_1 and X_2 are isomorphic n-coverings as $\phi_1\phi_2^{-1}$ is defined over K. Finally any cocycle $c \in Z^1(G_K, A[n])$ naturally corresponds to a cocycle in $Z^1(G_K, A)$. By Proposition 1.5.3, it corresponds to a principal homogeneous space X with $\phi : X \to A$ such that $\phi(\phi^{-1})^\sigma$ equals c. This implies that $[n] \circ \phi$ is defined over K which makes $(X, [n] \circ \phi)$ an n-covering mapping to c.

□

An example of the above correspondence is the following corollary.

Corollary 1.5.11. *Let A be an abelian variety defined over K. Let $P \in A(K)$ represent an element in $A(K)/nA(K)$, denoted by $[P]$. Then the image of $[P]$ under the connecting map $A(K)/nA(K) \to H^1(G_K, A[n])$ corresponds to the two-covering $(A, [n] \circ \tau_{-Q})$, where Q is any point of A such that $nQ = P$.*

Proof. The definition of the connecting map shows that $[P] \in A(K)/nA(K)$ maps to the cocycle class represented by $\sigma \mapsto \sigma(Q) - Q$, where Q is a point of A such that $nQ = P$. Note that this image is independent of the choice of Q. We know $\tau_{-Q} \circ \sigma(\tau_{-Q}^{-1}) = \tau_{\sigma(Q)-Q}$, and we are done by Proposition 1.5.10.

□

Remark 1.5.12. It is well-known for X the n-covering of an abelian variety A corresponding to the cocycle class $\epsilon \in H^1(G_K, A[n])$, X contains a K-rational point if and only if ϵ is in the image of the connecting map $A(K)/nA(K) \to H^1(G_K, A[n])$. This can be seen by the exact sequence $0 \to A(K)/nA(K) \to H^1(G_K, A[n]) \to H^1(G_K, A)$ and Corollary 1.5.6. A proof of this in the case $n = 2$ and $A = J$ can also be found in [FTvL12, Proposition 2.15].

1.6 Brauer-Severi Diagrams

In this section, we introduce the Brauer-Severi diagrams for the Jacobian variety J of a genus two curve. Recall that the divisor class of $n\Theta$ is defined over K for any positive even integer n as in Remark 1.2.3.

For a fixed even integer $n \geq 2$, a *Brauer-Severi* diagram $[X \to S]$ is a morphism defined over K from a principal homogeneous space X for J to a variety S such that there exist an isomorphism of torsors ϕ and an isomorphism of varieties ψ making the following diagram commute:

$$\begin{array}{ccc} X & \longrightarrow & S \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \psi} \\ J & \xrightarrow{|n\Theta|} & \mathbb{P}^{n^2-1}, \end{array} \tag{1.6.1}$$

and in particular, the variety S is a *Brauer-Severi* variety i.e. a variety that is isomorphic to a projective space over $\bar{K}$.

We call the Brauer-Severi diagram $[J \xrightarrow{|n\Theta|} \mathbb{P}^{n^2-1}]$, the *base Brauer-Severi diagram*. Two Brauer-Severi diagrams $[X_1 \to S_1]$ and $[X_2 \to S_2]$ are isomorphic if there exist an isomorphism of torsors f and an isomorphism of varieties g making the following diagram commutes:

$$\begin{array}{ccc} X_1 & \longrightarrow & S_1 \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} \\ X_2 & \longrightarrow & S_2. \end{array}$$

It can be shown that the isomorphism classes of Brauer-Severi diagrams are parameterized by $H^1(G_K, J[n])$. The elliptic curves case is done in [CFO+08, Proposition 1.19], and here we state and prove the result for Jacobians of genus two curves.

Proposition 1.6.1. *There is a bijection between the set of isomorphism classes of Brauer-Severi diagrams and the set $H^1(G_K, J[n])$.*

Proof. Let $[X \to S]$ be a Brauer-Severi diagram. Then there exist ϕ, ψ such that (1.6.1) commutes where $\phi : X \to J$ is an isomorphism of torsors. By Proposition 1.5.3, we know that $\phi(\phi^{-1})^\sigma = \tau_{P_\sigma}$ for some $P_\sigma \in J$ and $(\sigma \mapsto P_\sigma)$ is a cocycle in $Z^1(G_K, J)$. For a fixed σ, we have

$$\begin{array}{ccc} J & \xrightarrow{|n\Theta|} & \mathbb{P}^{n^2-1} \\ \downarrow{\scriptstyle \phi(\phi^{-1})^\sigma} & & \downarrow{\scriptstyle \psi(\psi^{-1})^\sigma} \\ J & \xrightarrow{|n\Theta|} & \mathbb{P}^{n^2-1}, \end{array}$$

which implies that $(\phi(\phi^{-1})^\sigma)^*(n\Theta) \sim n\Theta$. Hence, $P_\sigma \in J[n]$ and $(\sigma \mapsto P_\sigma)$ is a cocycle in $Z^1(G_K, J[n])$. Suppose there also exist ϕ', ψ' making (1.6.1) commute. Then we have the following commutative diagram:

$$\begin{array}{ccccc} J & \times & J & \xrightarrow{+} & J \\ \downarrow{\scriptstyle =} & & \downarrow{\scriptstyle \phi'^{-1}} & & \downarrow{\scriptstyle \phi'^{-1}} \\ J & \times & X & \longrightarrow & X \\ \downarrow{\scriptstyle =} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi} \\ J & \times & J & \xrightarrow{+} & J \end{array}$$

Since $\phi\phi'^{-1}$ is an isomorphism as torsors, by Lemma 1.5.2 we get $\phi\phi'^{-1} = \tau_P$ for some $P \in J$. In fact, we have $P \in J[n]$ as $\phi\phi'^{-1}$ is an automorphism of base Brauer-Severi diagram. This implies that the cocycles correspond to different choices of ϕ differ by a coboundary in $B^1(G_K, J[n])$. We also check that isomorphic Brauer-Severi diagrams indeed correspond to the same element in

$H^1(G_K, J[n])$.

Suppose $[X_1 \to S_1], [X_2 \to S_2]$ are two Brauer-Severi diagrams that map to the same element in $H^1(G_K, J[n])$. We have $X_1 \xrightarrow{\phi_1} J, X_2 \xrightarrow{\phi_2} J$ isomorphisms as torsors. By composing ϕ_2 with τ_Q for some $Q \in J[n]$, we can assume $\phi_1(\phi_1^{-1})^\sigma = \phi_2(\phi_2^{-1})^\sigma$ for all $\sigma \in G_K$ which implies $[X_1 \to S_1], [X_2 \to S_2]$ are isomorphic over K. For surjectivity, let $c \in Z^1(G_K, J[n])$ be a cocycle and consider its image in $Z^1(G_K, J)$. By Proposition 1.5.3, there exist a torsor X of J and an isomorphism as torsors $\phi : X \to J$ such that $(\sigma \mapsto \phi(\phi^{-1})^\sigma)$ gives c. This implies $\phi^*(n\Theta) \sim (\phi^\sigma)^*(n\Theta)$ via the principal polarization and so the divisor class of $\phi^*(n\Theta)$ is defined over K. Hence, it induces a morphism $X \to S$ over K which makes $[X \xrightarrow{|\phi^*(n\Theta)|} S]$ a Brauer-Severi diagram as required.

□

The following proposition gives the relationship between n-coverings of J and Brauer-Severi diagrams.

Proposition 1.6.2. *Let (X, π) be an n-covering of J, with $\phi \circ [n] = \pi$. Then the map $|\phi^*(n\Theta)|$ is defined over K and we have a Brauer-Severi diagram $[X \xrightarrow{|\phi^*(n\Theta)|} S]$. In particular, if (X, π) corresponds to a Selmer element via the correspondence in Proposition 1.5.10, then we have that the Brauer-Severi variety S is $\mathbb{P}^{n^2-1}$.*

Proof. Since (X, π) is a n-covering of J, by Proposition 1.5.10, we have that for each $\sigma \in G_K$, $\phi \circ (\phi^{-1})^\sigma = \tau_P$ for some $P \in J[n]$. The principal polarization gives $\tau_P^*(n\Theta) \sim n\Theta$ which implies that $\phi^*(n\Theta) \sim (\phi^\sigma)^*(n\Theta)$, hence the morphism $|\phi^*(n\Theta)|$ is defined over K.

Now if (X, π) corresponds to a Selmer element, then X everywhere locally has a point by Remark 1.5.12, and hence S everywhere locally has a point. Since Hasse principle holds for Brauer-Severi varieties by [CM96, Corollary 2.6], we know that S has a point over K and hence it is $\mathbb{P}^{n^2-1}$ by [GS06, Therem 5.1.3].

□

We now make some observations and notation in the case where $n = 2$.

Remark 1.6.3. Let $\epsilon \in \mathrm{Sel}^2(J)$, and let $(J_\epsilon, \pi_\epsilon)$ denote the 2-covering corresponding to ϵ. There exists an isomorphism ϕ_ϵ defined over $\bar{K}$ such that $[2] \circ \phi_\epsilon = \pi_\epsilon$ is a morphism defined over K. Then, by Proposition 1.6.2, we have the following commutative diagram:

$$\begin{array}{ccc} J_\epsilon & \xrightarrow{|\phi_\epsilon^*(2\Theta)|} & \mathcal{K}_\epsilon \subset \mathbb{P}^3 \\ \downarrow{\scriptstyle \phi_\epsilon} & & \downarrow{\scriptstyle \psi_\epsilon} \\ J & \xrightarrow{|2\Theta|} & \mathcal{K} \subset \mathbb{P}^3. \end{array} \tag{1.6.2}$$

We denote the image of J_ϵ under the morphism induced by $|\phi_\epsilon^*(2\Theta)|$ by $\mathcal{K}_\epsilon$, called the *twisted Kummer surface* corresponding to ϵ and ψ_ϵ is a linear isomorphism $\mathbb{P}^3 \to \mathbb{P}^3$ defined over $\bar{K}$. This commutative diagram will become essential in the later parts of the thesis.

Notation 1.6.4. Suppose $(J_\epsilon, \pi_\epsilon)$ is the 2-covering of J corresponding to $\epsilon \in H^1(G_K, J[2])$. Via the involution $[-1] : P \mapsto -P$ on J, we have an induced involution on J_ϵ denoted by ι_ϵ such that $\phi_\epsilon \circ \iota_\epsilon = [-1] \circ \phi_\epsilon$, where $[2] \circ \phi_\epsilon = \pi_\epsilon$. Note, by Lemma 1.5.8, we know ι_ϵ is independent of the choice of ϕ_ϵ. Since $[2] \circ \phi_\epsilon = \pi_\epsilon$ implies $[2] \circ \phi_\epsilon^\sigma = \pi_\epsilon$ for any $\sigma \in G_K$, we have ι_ϵ is defined over K. Moreover, the degree 2 morphism $J_\epsilon \xrightarrow{|\phi_\epsilon^*(2\Theta)|} \mathcal{K}_\epsilon \subset \mathbb{P}^3$ in (1.6.2) is precisely the quotient by ι_ϵ and an alternative definition of $\mathcal{K}_\epsilon$ is the quotie nt of J_ϵ by ι_ϵ. We sometimes call a function g on J_ϵ even if it is invariant under ι_ϵ and odd if $g \circ \iota_\epsilon = -g$.

1.7 The Weil Pairing

We start by stating the theorem of the Weil pairing. This is taken from [Mil08, Chapter 1 Section 13] (Cf. [Mum70, Section 20, page 184]).

Theorem 1.7.1. *(The Weil Pairing) For a principally polarized abelian variety (A, λ) defined over a field K, and an integer n not divisible by the characteristic of K. Let $A^\vee$ denote its dual abelian variety. There exists a canonical pairing:*

$$e_n : A[n] \times A^\vee[n] \to \bar{K}^*,$$

that is bilinear, nondegenerate, and Galois equivariant.

Via the polarization λ, we get a pairing

$$e_n^\lambda : A[n] \times A[n] \to \bar{K}^*,$$

where $e_n^\lambda(a, b) = e_n(a, \lambda(b))$. Moreover, e_n^λ is bilinear, anti-symmetric, nondegenerate, and Galois equivariant.

Note that since e_n, e_n^λ are nondegenerate and bilinear, we know that the image of e_n and the image of e_n^λ are in fact $\mu_n(\bar{K}^*)$.

The Weil pairing e_n can be defined explicitly as follows. For simpicity, we assume K is algebraically closed. Let $a \in A[n], a' \in A^\vee[n] \subset \mathrm{Pic}^0(A)$. Suppose a' is represented by the divisor D on A. Then $n_A^* D$ is linearly equivalent to nD which is linearly equivalent to 0, where $n_A : A \xrightarrow{x \mapsto nx} A$. Therefore, there are rationals functions f, g on A such that $nD = (f)$ and $n_A^* D = (g)$. We have

$$\mathrm{div}(f \circ n_A) = n_A^*(\mathrm{div}(f)) = n_A^*(nD) = n(n_A^* D) = \mathrm{div}(g^n).$$

Hence, $g^n/(f \circ n_A)$ is a constant function c on A. Moreover,

$$g(x+a)^n = cf(nx+na) = cf(nx) = g(x)^n,$$

which implies that $g/(g \circ \tau_a)$ is a function on A whose n^{th} power is 1. This implies that it is an n^{th} root of unity in the function field of A and can be identified with an element in $\mu_n(\bar{K}^*) \subset \bar{K}^*$. Define $e_n(a, a') = g/(g \circ \tau_a)$.

For a principally polarized abelian variety with a fixed polarization λ, we sometimes denote e_n^λ by e_n for simplicity. We quote the following well-known result on the n-torsion group of an abelian variety A.

Lemma 1.7.2. [Mil08, Chapter 1 Remark 7.3] *Let A be an abelian variety of dimension d. We have $A[n] \cong \mu_n^{2d}$ which implies that $|A[n]| = n^{2d}$.*

1.7.1 Properties of the Weil pairing

In this section, we state some properties of the Weil pairing that is needed in the thesis. First, we have the following lemma that shows the compatibility of the Weil pairing.

Lemma 1.7.3. [Mil08, Chapter 1 Lemma 13.1] *Let (A, λ) be a principally polarized abelian variety defined over a field K, and m, n be integers not divisible by the characteristic of K. Then for all $a \in A[mn]$ and $a' \in A^\vee[mn]$,*

$$e_{mn}(a, a')^m = e_n(ma, ma').$$

Hence, via the polarization λ, for all $a, b \in A[mn]$,

$$e_{mn}^\lambda(a, b)^m = e_n^\lambda(ma, mb).$$

The following properties and notation related to the Weil pairing are used in the later chapters.

Remark 1.7.4.

(i) Let $\cup_n : C^1(G_K, A[n]) \times C^1(G_K, A[n]) \to C^2(G_K, \bar{K}^*)$ denote the cup product pairing associated to e_n. We know the cup product of two cocycles is a cocycle and the cup product is trivial if one of the arguments is a coboundary. This implies that the cup product naturally extends to a pairing $H^1(G_K, A[n]) \times H^1(G_K, A[n]) \to H^2(G_K, \bar{K}^*)$. We sometimes also denote this induced pairing by $\cup_n$ when the context is clear.

(ii) By Lemma 1.7.3, we know that $(a \cup_{mn} b)^m = ma \cup_n mb$ for all $a, b \in C^1(G_K, A[mn])$.

(iii) In the case where K is a number field, we let $\cup_n$ denote the cup product associated to e_n over K and $\cup_{n,v}$ denote the cup product associated to e_n over K_v for each place v of K.

We quote the following lemma on Tate local duality which gives some properties of the cup product associated to e_n.

Lemma 1.7.5. [Sko, Lemma 2.7 and Complements(1)] *Let A be a principally polarized abelian variety defined over a local field K. Consider the subgroup $A(K)/nA(K) \subset H^1(G_K, A[n])$ via the connecting map δ_n induced by $A \xrightarrow{n} A$ as in Notation 1.4.1. We have that $A(K)/nA(K)$ is orthogonal to itself with respect to the cup product*

$$\cup_n : H^1(G_K, A[n]) \times H^1(G_K, A[n]) \to H^2(G_K, \bar{K}^*) \cong Br(K).$$

Moreover, $A(K)/nA(K)$ is the exact annihilator of itself with respect to the pairing that is the composition of the cup product $\cup_n$ above and the local invariant map:

$$H^1(G_K, A[n]) \times H^1(G_K, A[n]) \to \mathbb{Z}/n\mathbb{Z}$$

.

1.7.2 Galois action on $J[2]$ and the Weil pairing

In this section, we discuss the Weil pairing on $J[2] \times J[2]$ when J is the Jacobian variety of a genus two curve. We relate this with the action of the Galois group G_K on $J[2]$. First, we have the explicit formula for the Weil pairing which is used in the later computations.

Lemma 1.7.6. [CF96, Chapter 3, Section 3] *Let J be the Jacobian variety of a genus two curve. Suppose $\{P_1, P_2\}$ and $\{Q_1, Q_2\}$ represent $P, Q \in J[2]$ where P_1, P_2, Q_1, Q_2 are Weierstrass points, then*

$$e_2(P, Q) = (-1)^{|\{P_1,P_2\} \cap \{Q_1,Q_2\}|}.$$

Now recall that our genus two curve $\mathcal{C}$ is defined by $y^2 = f(x)$ and f is a polynomial of degree 6 defined over K with roots $\omega_1, ..., \omega_6$. We let L_1 denote the splitting field of f and let $\mathrm{Gal}(f)$ denote the Galois group of L_1/K.

Let $M = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$. The *symplectic group* is defined as

$$\mathrm{Sp}_4(\mathbb{F}_2) = \{A \in \mathrm{Mat}_4(\mathbb{F}_2) : A^T M A = M\},$$

and it can be checked that $|\mathrm{Sp}_4(\mathbb{F}_2)| = 720$.

Since $J[2] \cong (\mathbb{Z}/2\mathbb{Z})^4$ by Lemma 1.7.2, we can view it as $\mathbb{F}_2$-vector space of dimension 4. Recall Remark 1.2.1. In particular, we can pick a set of basis P_1, P_2, P_3, P_4 for $J[2]$ such that the Weil pairing matrix under this basis is precisely represented by M. For example, we can let $P_1 = \{(\omega_1, 0), (\omega_2, 0)\}, P_2 = \{(\omega_3, 0), (\omega_4, 0)\}, P_3 = \{(\omega_1, 0), (\omega_5, 0)\}, P_4 = \{(\omega_3, 0), (\omega_6, 0)\}$. Note here we identify $(\mathbb{F}_2, +)$ with $(\mu_2, \times)$. Since the Weil pairing is Galois equivariant and Galois acts trivially on $\{0, 1\}$, every element $\sigma \in G_K$ induces a change of basis on $J[2]$, as a $\mathbb{F}_2$-vector space, that preserves the Weil pairing. This gives a group homomorphism $G_K \to \mathrm{Sp}_4(\mathbb{F}_2)$ and we have the following lemma.

Lemma 1.7.7.

(i) $Sp_4(\mathbb{F}_2) \cong S_6$.

(ii) $G_K \to Sp_4(\mathbb{F}_2)$ *is surjective if and only if* $Gal(f) = S_6$.

Proof. Let Ω denote the set of six roots of f. We know $\mathrm{Aut}(\Omega) \cong S_6$. By Lemma 1.7.6, we observe elements in $\mathrm{Aut}(\Omega)$ naturally induce change of basis matrices on $J[2]$, viewed as a $\mathbb{F}_2$-vector space, that preserve the Weil pairing. This implies that they give elements in $\mathrm{Sp}_4(\mathbb{F}_2)$. We can check that this induced map is an injective homomorphism. Then by size comparison, we know that it is in fact an isomorphism which gives (i). Hence, we have the following commutative diagram of group homomorphisms.

$$\begin{array}{ccc} G_K & \longrightarrow & \mathrm{Aut}(\Omega) \\ & \searrow & \downarrow \cong \\ & & \mathrm{Sp}_4(\mathbb{F}_2) \end{array}$$

From the commutative diagram above, we know the map $G_K \to \mathrm{Sp}_4(\mathbb{F}_2)$ is surjective if and only if $G_K \to \mathrm{Aut}(\Omega)$ is surjective which is equivalent to $\mathrm{Gal}(f) = S_6$. Hence (ii) holds.

□

1.8 Definition of the Cassels-Tate Pairing

In this section, we give two equivalent definitions of the Cassels-Tate pairing (CTP) on a principally polarized abelian variety A defined over a number field K. Generally, the Cassels-Tate pairing is defined and studied on the Tate-Shafarevich group $Ш(A)$. In this thesis, we will mainly be working on the Cassels-Tate pairing on the Selmer groups where the definition naturally follows, see Remark 1.8.7(iv), and more details are discussed later in this section. Most material comes from [PS99].

Theorem 1.8.1. *Let (A, λ) be a principally polarized abelian variety defined over a number field K. There is an anti-symmetric bilinear pairing*

$$Ш(A) \times Ш(A) \longrightarrow \mathbb{Q}/\mathbb{Z},$$

that is nondegerate after quotienting out the maximal divisible subgroup.

Remark 1.8.2. If A is an elliptic curve, Cassels [Cas62] proved that the pairing is in fact alternating. If $Ш(E)$ is finite, which is conjectured to always be the case, then this implies that the order of $Ш(E)$ is a square. In [Fla90], Flach proved that for principally polarized abelian varieties, the pairing is always antisymmetric. In [PS99], Poonen and Stoll gave explicit examples to show the pairing need not be alternating and the order of $Ш(A)$ need not be a square even in the case where A is Jacobian variety of a curve defined over $\mathbb{Q}$.

We now have the following lemma for a special case when A is the Jacobian variety J of a genus two curve $\mathcal{C}$ defined over K.

Lemma 1.8.3. *If $\mathcal{C}$ has a K-rational point, the Cassels-Tate pairing on $Ш(J) \times Ш(J)$ is alternating.*

Proof. Recall that J is principally polarized via a theta divisor Θ and the divisor class of a theta divisor is in $H^0(G_K, \mathrm{NS}(J))$ as discussed in Remark 1.2.2. Consider the long exact sequence induced by the short exact sequence $0 \to J^\vee \to \mathrm{Pic}(J) \to \mathrm{NS}(J) \to 0$,

$$0 \to J^\vee(K) \to H^0(G_K, \mathrm{Pic}(J)) \to H^0(G_K, \mathrm{NS}(J)) \to H^1(G_K, J^\vee).$$

Since $\mathcal{C}$ has a K-rational point, the equivalence class of Θ in $H^0(G_K, \mathrm{NS}(J))$ has a lift in $H^0(G_K, \mathrm{Pic}(J))$ and hence is mapped to 0 in $H^1(G_K, J^\vee)$. Then the result in the lemma follows directly from [PS99, Corollary 7].

□

We note that, by Remark 1.5.5, it suffices to define the Cassels-Tate pairing on $Ш(A)[n]$ for every positive integer n.

1.8.1 The Weil pairing definition of the CTP

Let (A, λ) be a principally polarized abelian variety defined over a number field K. We now define the Cassels-Tate pairing $\langle a, a' \rangle_{CT}$ for $a, a' \in Ш(A)[n]$. We let $b, b' \in \mathrm{Sel}^n(A) \subset H^1(G_K, A[n])$ denote the lifts of a, a' and are represented by the cocycles $t, t' \in Z^1(G_K, A[n])$.

Let $s \in C^1(G_K, A[n^2])$ be such that $ns = t$. This implies that the cocycle ds takes value in $A[n]$ as $nds = dt = 0$. Let $\cup_n : C^2(G_K, A[n]) \times C^1(G_K, A[n]) \to C^3(G_K, \bar{K}^*)$ denote the cup-product pairing associated to e_n. Now $ds \cup_n t'$ represents an element in $H^3(G_K, \bar{K}^*)$. Since K is a number field, we know that $H^3(G_K, \bar{K}^*) = 0$ as proved in [CF67, Chapter VII, Section 11.4]. Therefore, there exists $r \in C^2(G_K, \bar{K}^*)$ such that $dr = -ds \cup_n t'$.

Now let v be a place of K. Since $a_v = 0$, there exists $Q_v \in A(\bar{K}_v)$ such that $d(nQ_v)$ equals the image of t_v in $Z^1(G_{K_v}, A(\bar{K}_v))$. Let $c_v = dQ_v \in Z^1(G_{K_v}, A[n^2])$. We get that $c_v - s_v$ takes value in $A[n]$ as $n(c_v - s_v) = d(nQ_v) - t_v = 0$.

Let $\cup_{n,v} : C^1(G_{K_v}, A[n]) \times C^1(G_{K_v}, A[n]) \to C^2(G_{K_v}, \bar{K_v}^*)$ denote the cup-product pairing associated to e_n. Since c_v and t'_v are both cocycles, $d((c_v - s_v) \cup_{n,v} t'_v) = -ds_v \cup_{n,v} t'_v = dr_v$. Hence, $((c_v - s_v) \cup_{n,v} t'_v) - r_v \in C^2(G_{K_v}, \bar{K_v}^*)$ is a cocycle representing an element $\eta_v \in H^2(G_{K_v}, \bar{K_v}^*)$. Via the invariant map $H^2(G_{K_v}, \bar{K_v}^*) \cong \mathrm{Br}(K_v) \xrightarrow{\mathrm{inv}_v} \mathbb{Q}/\mathbb{Z}$, we define the Cassels-Tate pairing of a and a' as follows:

$$\langle a, a' \rangle_{CT} := \sum_v \mathrm{inv}_v(\eta_v).$$

Sometimes, we refer to $\mathrm{inv}_v(\eta_v)$ above as the local Cassels-Tate pairing between $a, a' \in Ш(A)[n]$, for a place v of K. We now state and prove the proposition below to show that the Weil pairing definition of the Cassels-Tate pairing given above is well-defined. This is explained in [PS99] but here we prove it directly and give more details.

Proposition 1.8.4. *The Weil pairing definition of the Cassels-Tate pairing defined above is independent of all the choices we make.*

Proof. This proof follows the notation in the Weil pairing definition of the Cassels-Tate pairing as above. Fix $a, a' \in Ш(A)[n]$. We will show that the Weil pairing definition of $\langle a, a' \rangle_{CT}$ is independent of the choices of $b, b' \in \mathrm{Sel}^n(A), t, t' \in Z^1(G_K, A[n]), s \in C^1(G_K, A[n^2]), r \in C^2(G_K, \bar{K}^*)$ and $Q_v \in A(\bar{K}_v)$ for each place v.

Step 1: In this step, we fix $b, b' \in \mathrm{Sel}^n(A), t, t' \in Z^1(G_K, A[n])$ and show the independence of $s \in C^1(G_K, A[n^2]), r \in C^2(G_K, \bar{K}^*)$ and $Q_v \in A(\bar{K}_v)$ for each

place v.

We first fix the choices of s, Q_v and suppose there exist $r, \tilde{r} \in C^2(G_K, \bar{K}^*)$ such that $dr = d\tilde{r} = -ds \cup_n t'$. Then $\tilde{r} = r + x$ for some $x \in Z^2(G_K, \bar{K}^*)$ as $dx = 0$. Let $\eta, \tilde{\eta} \in H^2(G_{K_v}, \bar{K_v}^*)$ be represented by $((c_v - s_v) \cup_{n,v} t'_v) - r_v, ((c_v - s_v) \cup_{n,v} t'_v) - \tilde{r_v} \in C^2(G_{K_v}, \bar{K_v}^*)$ respectively. Then $\tilde{\eta} - \eta$ is represented by the cocycle $-x_v$. But by the exact sequence $0 \to \mathrm{Br}(K) \to \bigoplus_v \mathrm{Br}(K_v) \xrightarrow{\sum_v \mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \to 0$, we get $\sum_v \mathrm{inv}_v(x_v) = 0$ as required.

Now we fix the choice of Q_v and suppose that there exist $s, \tilde{s} \in C^1(G_K, A[n^2])$ such that $ns = n\tilde{s} = t$. This implies that $\tilde{s} = s + y$ for some $y \in C^1(G_K, A[n])$. Since we have shown the definition is independent of the choice of r, we pick any $r, \tilde{r} \in C^2(G_K, \bar{K}^*)$ such that $dr = -ds \cup_n t', d\tilde{r} = -d\tilde{s} \cup_n t' = dr - dy \cup_n t'$. Let $\eta, \tilde{\eta} \in H^2(G_{K_v}, \bar{K_v}^*)$ be represented by $((c_v - s_v) \cup_{n,v} t'_v) - r_v, ((c_v - \tilde{s_v}) \cup_{n,v} t'_v) - \tilde{r_v} \in C^2(G_{K_v}, \bar{K_v}^*)$ respectively. Then $\tilde{\eta} - \eta$ is represented by the cocycle $-y_v \cup_{n,v} t'_v - \tilde{r_v} + r_v = (-y \cup_n t' - \tilde{r} + r)_v$. Note that $d(-y \cup_n t' - \tilde{r} + r) = 0$. Using the same argument as the previous case, we get $\sum_v \mathrm{inv}_v((-y \cup_n t' - \tilde{r} + r)_v) = 0$ as required.

Then we show the independence of the choice of Q_v for each place v, fixing s and r. Suppose there exist $Q_v, \tilde{Q_v} \in A(\bar{K_v})$ for some place v such that $d(nQ_v) = d(n\tilde{Q_v})$ which is equal to the image of t_v in $Z^1(G_{K_v}, A(\bar{K_v}))$. Hence $n\tilde{Q_v} = nQ_v + z_v$ for some $z_v \in A(K_v)$ as $dz_v = 0$. Let $z'_v \in A(\bar{K_v})$ satisfy $\tilde{Q_v} = Q_v + z'_v$ and $nz'_v = z_v$. Let $c_v = dQ_v, \tilde{c_v} = d\tilde{Q_v}$ in $Z^1(G_{K_v}, A[n^2])$ and $\eta, \tilde{\eta} \in H^2(G_{K_v}, \bar{K_v}^*)$ be represented by $((c_v - s_v) \cup_{n,v} t'_v) - r_v, ((\tilde{c_v} - s_v) \cup_{n,v} t'_v) - r_v \in C^2(G_{K_v}, \bar{K_v}^*)$ respectively. Hence, $\tilde{c_v} = c_v + dz'_v$ and $\tilde{\eta_v} - \eta_v$ is represented by the cocycle $dz'_v \cup_{n,v} t'_v$. Recall that $z_v \in A(K_v)$ which implies dz'_v represents $\delta_n(z_v) \in H^1(G_{K_v}, A[n])$. Also since t' represents a Selmer element, there exists a $T_v \in A(K_v)$ such that t'_v represents $\delta_n(T_v) \in H^1(G_{K_v}, A[n])$. Recall δ_n corresponds to $A \xrightarrow{[n]} A$ as in Notation 1.4.1. Hence, the cup product $dz'_v \cup_{n,v} t'_v$ represents the trivial cohomology element by Lemma 1.7.5, as required.

Step 2: In this step, we fix t', b' and show the independence of t and b. Suppose there exist $t, \tilde{t} \in Z^1(G_K, A[n])$ such that both their images in $Z^1(G_K, A)$ represent $a \in H^1(G_K, A)$. Let $\tilde{t} = t + dw$, for some $w \in A(\bar{K})$ such that $nw \in A(K)$. Note that from the first part of the proof, we know the definition is independent of the choices of s, r and Q_v. Pick any $s \in C^1(G_K, A[n^2])$ such that $ns = t$, let $\tilde{s} = s + dw_1$ for some $w_1 \in A(\bar{K})$ such that $nw_1 = w$. This implies $n\tilde{s} = t + dw = \tilde{t}$ as required. So $ds = d\tilde{s}$ which means can pick $\tilde{r} = r$, where $r, \tilde{r} \in C^2(G_K, \bar{K}^*)$ satisfying $dr = -ds \cup_n t', d\tilde{r} = -d\tilde{s} \cup_n t'$ respectively. Then for a place v of K, pick any $Q_v \in A(\bar{K_v})$ such that $dnQ_v = t_v$. Let $\tilde{Q_v} = Q_v + w_{1,v}$ so $dn\tilde{Q_v} = t_v + dw_v = \tilde{t_v}$ as required. Let $c_v = dQ_v, \tilde{c_v} = d\tilde{Q_v}$, then $\tilde{c_v} - c_v = dw_{1,v} = \tilde{s_v} - s_v$. Let $\eta, \tilde{\eta} \in H^2(G_{K_v}, \bar{K_v}^*)$ be represented by $((c_v - s_v) \cup_{n,v} t'_v) - r_v, ((\tilde{c_v} - \tilde{s_v}) \cup_{n,v} t'_v) - \tilde{r_v} \in C^2(G_{K_v}, \bar{K_v}^*)$ respectively. Since $\tilde{c_v} - \tilde{s_v} = c_v - s_v$ and $\tilde{r} = r$, we get $\tilde{\eta_v} = \eta_v$.

Step 3: In this step, we fix t, b and show the independence of t' and b'. Suppose there exist $t', \tilde{t'} \in Z^1(G_K, A[n])$ such that both their images in $Z^1(G_K, A)$ represent $a' \in H^1(G_K, A)$. This implies that there exists $R \in A(K)$ such that $\delta_n(R) \in H^1(G_K, A[n])$ is represented by $u = \tilde{t'} - t' \in Z^1(G_K, A[n])$. This implies that $u = dR_1$ for some $R_1 \in A(\bar{K})$ such that $nR_1 = R$. Note that from the first part of the proof, we know the definition is independent of the choices of s, r and Q_v. Let $r \in C^2(G_K, \bar{K}^*)$ be such that $dr = -ds \cup_n t'$ and define $\tilde{r} = r - s \cup_{n^2} u' \in C^2(G_K, \bar{K}^*)$ where $u' = dR_1'$ for some $R_1' \in A(\bar{K})$ such that $nR_1' = R_1$. This implies $nu' = u$. Then by Remark 1.7.4(ii) and the bilinearity of the Weil pairing, $ds \cup_{n^2} u' = ds \cup_n u$. Also $u' = dR_1'$ implies that $du' = 0$. Hence, $d\tilde{r} = dr - ds \cup_n u = -ds \cup_n \tilde{t'}$ as required. Let $\eta, \tilde{\eta} \in H^2(G_{K_v}, \bar{K_v}^*)$ be represented by $((c_v - s_v) \cup_{n,v} t_v') - r_v, ((c_v - s_v) \cup_{n,v} \tilde{t_v'}) - \tilde{r_v} \in C^2(G_{K_v}, \bar{K_v}^*)$ respectively. We get $\tilde{\eta} - \eta$ is represented by the cocycle $(c_v - s_v) \cup_{n,v} u_v + s_v \cup_{n^2,v} u_v'$. By Remark 1.7.4(ii) and the bilinearity of the Weil pairing, this cocycle is simplified to be $c_v \cup_{n^2,v} u_v'$. Recall that dnQ_v is the image of $t_v \in Z^1(G_{K_v}, A[n])$ in $Z^1(G_{K_v}, A)$, so $n^2(Q_v) = Q_v' \in A(K_v)$. Hence $c_v \cup_{n^2,v} u_v' = dQ_v \cup_{n^2,v} u_v'$ where dQ_v represents $\delta_{n^2}(Q_v')$ and u_v' represents $\delta_{n^2} R_v$. Then by Lemma 1.7.5, $c_v \cup_{n^2,v} u_v'$ represents the trivial cohomology element as required.

□

We will now give an alternative definition of the Weil pairing definition of the Cassels-Tate pairing on $Ш(A)[n] \times Ш(A)[n]$ in a special case.

Proposition 1.8.5. *Let $b, b' \in Sel^n(A)$ be lifts for $a, a' \in Ш(A)[n]$. Suppose there exists $b_1 \in H^1(G_K, A[n^2])$ such that $nb_1 = b$, induced by the map $A[n^2] \xrightarrow{[n]} A[n]$. The Weil pairing definition of $\langle a, a' \rangle_{CT}$ can be simplified.*

More explicitly, let v be a place of K and $P_v \in A(K_v)$ such that $\delta_n(P_v) = b_v \in H^1(G_{K_v}, A[n])$, where δ_n corresponds to the map $A \xrightarrow{[n]} A$ as in Notation 1.4.1. Then $\delta_{n^2}(P_v)$ and $b_{1,v}$ in $H^1(G_{K_v}, A[n^2])$ are both mapping to b_v, where δ_{n^2} corresponds to the map $A \xrightarrow{[n^2]} A$ as in Notation 1.4.1. Hence, define $\rho_v \in H^1(G_{K_v}, A[n])$ to be a lift of $\delta_{n^2}(P_v) - b_{1,v}$. See the commutative diagram below.

$$\begin{array}{ccccc}
A(K_v) & \xrightarrow{n} & A(K_v) & \xrightarrow{\delta_n} & H^1(G_{K_v}, A[n]) \\
\Big\| & & \Big\downarrow n & & \Big\downarrow \iota \; \rho_v \mapsto \delta_{n^2}(P_v) - b_{1,v} \\
A(K_v) & \xrightarrow[n^2]{} & A(K_v) & \xrightarrow{\delta_{n^2}} & H^1(G_{K_v}, A[n^2]) \\
\Big\downarrow n & & \Big\| & & \Big\downarrow n \; \delta_{n^2}(P_v) \mapsto b_v \;\; b_{1,v} \mapsto b_v \\
A(K_v) & \xrightarrow{n} & A(K_v) & \xrightarrow[\delta_n]{P_v \mapsto b_v} & H^1(G_{K_v}, A[n])
\end{array}$$

Define $\eta_v = \rho_v \cup_{n,v} b_v' \in H^2(G_{K_v}, \bar{K_v}^*)$. Note, here $\cup_{n,v} : H^1(G_{K_v}, A[n]) \times H^1(G_{K_v}, A[n]) \to H^2(G_{K_v}, \bar{K_v}^*)$ denotes the cup-product pairing associated to

e_n in the cohomology level.

Then we let

$$\langle a, a' \rangle_1 := \sum_v inv_v(\eta_v),$$

and we have $\langle a, a' \rangle_1 = \langle a, a' \rangle_{CT}$.

Furthermore, $\langle a, a' \rangle_1$ is independent of all the choices we make.

Proof. Since there exists $b_1 \in H^1(G_K, A[n^2])$ such that $nb_1 = b$, we know there exists $s \in Z^1(G_K, A[n^2])$ representing b_1 such that $ns = t \in Z^1(G_K, A[n])$ representing b. Then $ds = 0$, and hence we can pick $r = 0$ in the definition of $\langle a, a' \rangle_{CT}$. We also let $t' \in Z^1(G_K, A[n])$ denote a cocycle representing b'.

For each place v of K, we have $\delta_n(P_v) = b_v$. There exists $Q_v \in A(\bar{K}_v)$ such that $n^2(Q_v) = P_v$ and $d(nQ_v)$ equals the image of t_v in $Z^1(G_{K_v}, A(\bar{K}_v))$. Let $c_v = dQ_v \in Z^1(G_{K_v}, A[n^2])$, then c_v is a cocycle representing $\delta_{n^2}(P_v) \in H^1(G_{K_v}, A[n^2])$. We check that $c_v - s_v$ takes value in $A[n]$, and $[c_v - s_v] \in H^1(G_{K_v}, A[n])$ is a lift of $\delta_{n^2}(P_v) - b_{1,v} \in H^1(G_{K_v}, A[n^2])$.

Hence, to prove the two pairings are the same, it suffices to show that for $x_1, x_2 \in Z^1(G_{K_v}, A[n])$ such that their images in $H^1(G_{K_v}, A[n^2])$ represent the same element, then $x_1 \cup_{n,v} t'_v$ and $x_2 \cup_{n,v} t'_v$ represent the same element in $H^2(G_{K_v}, \bar{K_v}^*)$. We know there exists $w \in A(\bar{K}_v)[n^2]$ such that $dw = x_1 - x_2$. It suffices to show that $dw \cup_{n,v} t'_v$ represents the trivial element in $H^2(G_{K_v}, \bar{K_v}^*)$. Now using the similar argument as above but in a local field, there exists $P'_v \in A(K_v)$ such that $\delta_n(P'_v) = b'_v$. Hence $n\delta_{n^2}(P'_v) = b'_v$, which implies that there exists $c'_v \in Z^1(G_{K_v}, A[n^2])$ such that nc'_v and t'_v represent the same element in $H^1(G_{K_v}, A[n])$. So it suffices to prove $dw \cup_{n,v} nc'_v$ represents the trivial element in $H^2(G_{K_v}, \bar{K_v}^*)$. By the bilinearity of $\cup_{n,v}$ and Remark 1.7.4(ii), we have $dw \cup_{n,v} nc'_v = dw \cup_{n^2,v} c'_v$ which is indeed a coboundary element as required.

Furthermore, since $\langle\ ,\ \rangle_{CT}$ is independent of all the choices we make, $\langle\ ,\ \rangle_1$ is also independent of all the choices we make.

□

The lemma below shows that if all n-torsion points of the principally polarized abelian variety A are defined over K, then the condition of Proposition 1.8.5 is satisfied and hence the Weil pairing definition of the Cassels-Tate pairing is simplified.

Lemma 1.8.6. *Let (A, λ) be a principally polarized abelian variety defined over K of dimension d. Suppose that the n-torsion points of A are all defined over K. The following statements hold:*

(i) The map $H^2(G_K, A[n]) \xrightarrow{res} \prod_v H^2(G_{K_v}, A[n])$ *is injective.*

(ii) For any $b \in Sel^n(A)$*, there exists* $b_1 \in H^1(K, A[n^2])$ *mapping to* b*. (Note (ii) holds as long as (i) holds.)*

(iii) $Ш(A) \subset nH^1(G_K, A)$*. (Note (iii) holds as long as (i) holds.)*

Proof. Since the Weil pairing e_n is non-degenerate and Galois equivariant, the fact that all points in $A[n]$ are defined over K implies that $\mu_n(\bar{K}^*) \subset K$. By Lemma 1.7.2, we know $|A[n]| = n^{2d}$ and $A[n] \cong \mu_n^{2d}$. So, by Corollary 1.4.15, we have $H^2(G_K, A[n]) \cong (H^2(G_K, \mu_n))^{2d} \cong (\mathrm{Br}(K)[n])^{2d}$ and similarly $H^2(G_{K_v}, A[n]) \cong (\mathrm{Br}(K_v)[n])^{2d}$. Hence, via the injection of $\mathrm{Br}(K) \to \bigoplus_v \mathrm{Br}(K_v)$, we have $H^2(G_K, A[n]) \xrightarrow{res} \prod_v H^2(G_{K_v}, A[n])$ is injective which proves (i).

Now, consider the following commutative diagram of short exact sequences.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A[n] & \longrightarrow & A[n^2] & \xrightarrow{n} & A[n] & \longrightarrow & 0 \\ & & \downarrow{=} & & \downarrow{inc} & & \downarrow{inc} & & \\ 0 & \longrightarrow & A[n] & \longrightarrow & A & \xrightarrow{n} & A & \longrightarrow & 0 \end{array}$$

We then obtain the following commutating diagram of long exact sequences along the rows by taking Galois cohomology.

$$\begin{array}{ccccc} H^1(G_K, A[n^2]) & \xrightarrow{n} & H^1(G_K, A[n]) & \longrightarrow & H^2(G_K, A[n]) \\ \downarrow & & \downarrow{b \mapsto c} & & \downarrow{=} \\ H^1(G_K, A) & \xrightarrow{n} & H^1(G_K, A) & \longrightarrow & H^2(G_K, A[n]) \\ \downarrow{res} & & \downarrow{res} & & \downarrow{inj} \\ \prod_v H^1(G_{K_v}, A) & \xrightarrow{n} & \prod_v H^1(G_{K_v}, A) & \longrightarrow & \prod_v H^2(G_{K_v}, A[n]) \end{array}$$

Since $b \in \mathrm{Sel}^n(A)$, its image $c \in H^1(G_K, A)$ is locally trivial. Hence, its image is also trivial in $\prod_v H^2(G_{K_v}, A[n])$. Via the injectivity of the map $H^2(G_K, A[n]) \to \prod_v H^2(G_{K_v}, A[n])$, we get that $b \mapsto 0 \in H^2(G_K, A[n])$. Thus b has a lift $b_1 \in H^1(G_K, A[n^2])$. Hence (ii) holds. The same argument gives (iii).

□

1.8.2 The homogeneous space definition of the CTP

Let (A, λ) be an abelian variety defined over a number field K. Suppose a and $a' \in Ш(A)$. Via the polarization λ, we get $a' \mapsto b$ where $b = \lambda(a') \in Ш(A^\vee)$. Let X be the (locally trivial) principal homogeneous space defined over K representing a. Then $\mathrm{Pic}^0(X_{\bar{K}})$ is canonically isomorphic as a G_K-module to $\mathrm{Pic}^0(A_{\bar{K}}) = A^\vee(\bar{K})$. Therefore, we have that $b \in Ш(A^\vee) \subset H^1(G_K, A^\vee)$ now represents an element in $H^1(G_K, \mathrm{Pic}^0(X_{\bar{K}}))$.

Now consider the exact sequence:

$$0 \to \bar{K}(X)^*/\bar{K}^* \to \mathrm{Div}^0(X_{\bar{K}}) \to \mathrm{Pic}^0(X_{\bar{K}}) \to 0.$$

We can then map b to an element $b' \in H^2(G_K, \bar{K}(X)^*/\bar{K}^*)$ using the long exact sequence associated to the short exact sequence above. Since $H^3(G_K, \bar{K}^*) = 0$, b' has a lift $f' \in H^2(G_K, \bar{K}(X)^*)$ via the long exact sequence induced by the following short exact sequence:

$$0 \to \bar{K}^* \to \bar{K}(X)^* \to \bar{K}(X)^*/\bar{K}^* \to 0.$$

Next we show that $f'_v \in H^2(G_{K_v}, \bar{K}_v(X)^*)$ is the image of an element $c_v \in H^2(G_{K_v}, \bar{K}_v{}^*)$. This is because $b \in Ш(A^\vee)$ is locally trivial which implies its image b' is locally trivial. Then the statement is true by the exactness of the sequence.

We then can define

$$\langle a, b \rangle = \sum_v \mathrm{inv}_v(c_v) \in \mathbb{Q}/\mathbb{Z}.$$

So we have defined the Cassels-Tate pairing on $Ш(A) \times Ш(A) \to \mathbb{Q}/\mathbb{Z}$ by

$$\langle a, a' \rangle_{CT} := \langle a, \lambda(a') \rangle.$$

We sometimes refer to $\mathrm{inv}_v(c_v)$ above as the local Cassels-Tate pairing between $a, a' \in Ш(A)$ for a place v of K and we make the following remarks that are useful for the later chapters.

Remark 1.8.7.

(i) One can compute c_v by evaluating f'_v at a point in $X(K_v)$ provided that one avoids the zeros and poles of f'_v. Note that $X(K_v) \neq \emptyset$ as X is a locally trivial homogeneous space of A, see Corollary 1.5.6.

(ii) By [PS99, Propositions 32, 33, 34], we know the homogeneous space definition of the Cassels-Tate pairing is equivalent to the Weil pairing definition

of the pairing. Hence, by Proposition 1.8.4, the homogeneous space definition of the Cassels-Tate pairing is independent of all the choices we make.

(iii) By the equivalence of the two definitions, we know that the Cassels-Tate pairing on $Ш(A)[n] \times Ш(A)[n]$ is well-defined and compatible. More specifically, $\langle a, a' \rangle_{CT}$ is the same whether we treat $a, a' \in Ш(A)[n]$ or $Ш(A)[nm]$ for any positive integer m.

(iv) Via the map $\mathrm{Sel}^n(A) \to Ш(A)[n]$, the definition of the Cassels-Tate pairing on $Ш(A)[n] \times Ш(A)[n]$ naturally lifts to a pairing on $\mathrm{Sel}^n(A) \times \mathrm{Sel}^n(A)$.

1.9 Cassels-Tate Pairing and Rank Bound

By the Mordell-Weil Theorem, the set of K-rational points of an abelian variety A defined over a number field K, denoted by $A(K)$, is a finitely generated abelian group. This implies that the rank of $A(K)$, denoted by r, is finite. Computing the rank is difficult but there are ways to compute upper bounds. One standard method is descent calculation. In this section, we explain how the Cassels-Tate pairing can potentially improve the rank bound of an abelian variety obtained by a standard descent calculation. Also we assume K is a number field in this section, unless stated otherwise.

1.9.1 Selmer group and rank bound

Let $\phi : A \to B$ be an isogeny between two principally polarized abelian varieties defined over K. Recall we defined the ϕ-Selmer group of A and Tate-Shafarevich group of A in Definition 1.4.2. The short exact sequence $0 \to A[\phi] \to A \xrightarrow{\phi} B \to 0$ induces a long exact sequence of Galois cohomology which gives the exactness of

$$0 \to B(K)/\phi(A(K)) \xrightarrow{\delta} H^1(G_K, A[\phi]) \to H^1(G_K, A)[\phi] \to 0,$$

and we have the following exact sequences of abelian groups:

$$0 \to B(K)/\phi(A(K)) \xrightarrow{\delta} \mathrm{Sel}^{\phi}(A) \to Ш(A)[\phi] \to 0.$$

Now let $\widehat{\phi}$ denote the dual isogeny of ϕ. Similarly we have

$$0 \to A(K)/\widehat{\phi}(B(K)) \xrightarrow{\widehat{\delta}} \mathrm{Sel}^{\widehat{\phi}}(B) \to Ш(B)[\widehat{\phi}] \to 0.$$

Via the Mordell-Weil Theorem and the structure theorem, we deduce

$$\left|\frac{A(K)}{nA(K)}\right| = n^r |A(K)[n]|.$$

Since $|A(K)/nA(K)| \leq |\mathrm{Sel}^n(A)|$ by the above exact sequences, we get $n^r \leq |\mathrm{Sel}^n(A)|/|A(K)[n]|$. We now state and prove the following well-known result which relates the Selmer group and the rank bound of an abelian variety more generally.

Lemma 1.9.1. *Let $\phi : A \to B$ be an isogeny between two principally polarized abelian varieties defined over K with $\widehat{\phi}$ being is dual and $\phi \circ \widehat{\phi} = [n]$. Let r denote the rank of A. Then,*

$$n^r \leq \frac{|Sel^{\phi}(A)| \times |Sel^{\widehat{\phi}}(B)|}{|A(K)[\phi]| \times |B(K)[\widehat{\phi}]|}. \tag{1.9.1}$$

In particular, if $A = B$ and $\phi = [n]$,we have

$$n^r \leq \frac{|Sel^{n}(A)|}{|A(K)[n]|}.$$

Proof. We note that it suffices to prove (1.9.1). It can be checked that we have the following exact sequence:

$$\begin{aligned} 0 \to A(K)[\phi] \to A(K)[n] \xrightarrow{\phi} B(K)[\widehat{\phi}] \\ \to B(K)/\phi(A(K)) \xrightarrow{\widehat{\phi}} A(K)/nA(K) \to A(K)/\widehat{\phi}(B(K)) \to 0. \end{aligned}$$

Since $|B(K)/\phi(A(K))| \leq |\mathrm{Sel}^{\phi}(A)|$ and $|A(K)/\widehat{\phi}(B(K))| \leq |\mathrm{Sel}^{\widehat{\phi}}(B)|$, we have (1.9.1) as required.

□

1.9.2 Application of the Cassels-Tate pairing

In this section, we discuss the application of the Cassels-Tate pairing in bounding the rank of a principally polarized abelian variety A. Here, the Cassels-Tate pairing is defined on $\mathrm{Sel}^n(A) \times \mathrm{Sel}^n(A)$, as explained in Remark 1.8.7(iv). We first state a useful lemma followed by the proposition that explains the application of the Cassels-Tate pairing in the rank bound.

Lemma 1.9.2. *Let $\phi : A \to B$ be an isogeny between two principally polarized abelian varieties defined over K with $\widehat{\phi}$ being its dual and $\phi \circ \widehat{\phi} = [n]$. We*

have the following exact sequence from the short exact sequence of $0 \to A[\phi] \to A[n] \xrightarrow{\phi} B[\widehat{\phi}] \to 0$*:*

$$0 \to A[\phi](K) \to A[n](K) \xrightarrow{\phi} B[\widehat{\phi}](K) \to Sel^{\phi}(A) \to Sel^{n}(A) \to Sel^{\widehat{\phi}}(B).$$

Proof. It can be checked directly.

□

Proposition 1.9.3. *Let* A *be a principally polarized abelian variety. Suppose one of the following assumptions holds.*

(i) $Ш(A)$ *is finite;*

(ii) For any $b \in Sel^{n}(A)$*, there exists* $b_1 \in H^1(G_K, A[n^2])$ *mapping to* b*.*

Then carrying out an n*-descent and computing the Cassels-Tate pairing on* $Sel^{n}(A) \times Sel^{n}(A)$ *gives the same rank bound as obtained from a* n^2*-descent where* $Sel^{n^2}(A)$ *needs to be computed.*

More explicitly, the kernel of the Cassels-Tate pairing $\langle\ ,\ \rangle_{CT}$ *on* $Sel^{n}(A) \times Sel^{n}(A)$ *is equal to the image of the natural map* $\alpha : Sel^{n^2}(A) \to Sel^{n}(A)$ *induced from* $A[n^2] \xrightarrow{\cdot n} A[n]$*.*

Proof. First, we apply Lemma 1.9.2 on the multiplication by n map on A and we have the following exact sequence:

$$0 \to A[n](K) \to A[n^2](K) \to A[n](K) \to \mathrm{Sel}^{n}(A) \to \mathrm{Sel}^{n^2}(A) \xrightarrow{\alpha} \mathrm{Sel}^{n}(A).$$

We will show that the kernel of the Cassels-Tate pairing $\langle\ ,\ \rangle_{CT}$ on $\mathrm{Sel}^{n}(A) \times \mathrm{Sel}^{n}(A)$ is equal to the image of the natural map $\alpha : \mathrm{Sel}^{n^2}(A) \to \mathrm{Sel}^{n}(A)$ induced from $A[n^2] \xrightarrow{\cdot n} A[n]$. Then, via the above exact sequence, we know that carrying out an n-descent and computing the Cassels-Tate pairing on $\mathrm{Sel}^{n}(A) \times \mathrm{Sel}^{n}(A)$, together with computing $A[n](K)$ and $A[n^2](K)$, gives the size of $\mathrm{Sel}^{n^2}(A)$. This implies that we would get the same rank bound as obtained from a n^2-descent.

We note that $\mathrm{Im}\,\alpha \subset \ker\langle\ ,\ \rangle_{CT}$. Indeed, suppose $a = \alpha(b) \in \mathrm{Sel}^{n}(A)$ where $b \in \mathrm{Sel}^{n^2}(A)$. Denote the image of a in $Ш[n] \subset H^1(G_K, A)$ by a' and the image of b in $Ш[n^2] \subset H^1(G_K, A)$ by b'. Then we have $nb' = a'$ and $\langle a', c\rangle_{CT} = \langle nb', c\rangle_{CT} = \langle b', nc\rangle_{CT} = \langle b', 0\rangle_{CT} = 0$, for any $c \in Ш[n]$.

To prove $\ker\langle\ ,\ \rangle_{CT} \subset \mathrm{Im}\,\alpha$, it suffices to prove $(*)$: the kernel of the Cassels-Tate pairing on $Ш(A)[n] \times Ш(A)[n]$ is precisely $nШ(A) \cap Ш(A)[n]$. Indeed if $x \in \ker\langle\ ,\ \rangle_{CT}$, then its image $x' \in Ш(A)[n]$ is in the kernel of the Cassels-Tate pairing on $Ш(A)[n] \times Ш(A)[n]$. Hence, by $(*)$, there exists $y' \in Ш(A)[n^2]$ such that $ny' = x'$ and y' has a lift $y \in \mathrm{Sel}^{n^2}(A)$. This implies that $\alpha(y) = x + z$,

where z has a lift $z' \in A(K)/nA(K)$. Then by treating $z' \in A(K)/n^2A(K)$, we have $\alpha(y - \delta_{n^2}(z')) = x$ as required.

Suppose condition (i) holds, that is $Ш(A)$ is finite. The Cassels-Tate pairing $\langle\ ,\ \rangle_{CT}$ on $Ш(A) \times Ш(A)$ is non-degenerate by Theorem 1.8.1. In this case, we get an induced isomorphism $\Phi : Ш(A) \cong Ш(A)^* = \{\text{homomorphism } \phi : Ш(A) \to \bar{K}^*\}$. The statement (*) holds if the set $S := \{x \in Ш(A) | \langle x, y\rangle_{CT} = 0, \text{ for all } y \in Ш(A)[n]\}$ is equal to $nШ(A)$. We observe $nШ(A) \subset S$, so it suffices to show $|S| = |nШ(A)|$. This is indeed true as $S \cong \mathrm{Ann}_{Ш(A)[n]}(Ш(A)^*) = \{\phi \in Ш(A)^* \text{ such that } \phi \text{ restricted to } Ш(A)[n] \text{ is trivial}\}$ under Φ, and hence $|S| = |Ш(A)|/|Ш(A)[n]| = |nШ(A)|$ by the assumption of the finiteness of $Ш(A)$.

Now suppose condition (ii) holds. The proof of $\ker\langle\ ,\ \rangle_{CT} \subset \mathrm{Im}\,\alpha$ is the same as the proof in the elliptic curve case in [Fis03, Theorem 3] using Proposition 1.7.5.

□

We now make the following remarks on the application of the Cassels-Tate pairing in improving the rank bound of A obtained via standard descent calculations.

Remark 1.9.4.

(i) From the definition of the Cassels-Tate pairing, we know that if the element in $\mathrm{Sel}^n(A)$ has a lift in $A(K)/nA(K)$, then it will be in the kernel of the pairing. Hence, we can bound $n^r \leq |\ker\langle\ ,\ \rangle_{CT}|/|A(K)[n]|$ instead of $n^r \leq |\mathrm{Sel}^n(A)|/|A(K)[n]|$. This already implies that computing the Cassels-Tate pairing can potentially improve the rank bound obtained via carrying out a standard descent calculation. Under assumption (i) or (ii), Proposition 1.9.3 gives a more precise statement of this improvement. In particular, assumption (i) is conjectured to be always true.

(ii) We note that the results of Proposition 1.9.3 also hold in the case where $H^2(G_K, A[n]) \xrightarrow{res} \prod_v H^2(G_K, A[n])$ is injective which includes the case where all points in $A[n]$ are defined over K by Lemma 1.8.6. This can be argued by the following two ways. The assumption that $Ш(A)$ is finite (assumption(i)) is only used to prove the statement $(*)$ in the proof of the proposition above. From [Mil06, Chapter 1, Lemma 6.17], we know that the statement $(*)$ holds under the assumption that $Ш(A) \subset nH^1(G_K, A)$. Hence, by Lemma 1.8.6, the statement $(*)$ automatically holds in the case where $H^2(G_K, A[n]) \xrightarrow{res} \prod_v H^2(G_K, A[n])$ is injective. Or we can argue that, the injectivity of $H^2(G_K, A[n]) \xrightarrow{res} \prod_v H^2(G_K, A[n])$ implies assumption(ii) by Lemma 1.8.6.

1.10 More Results in Galois Cohomology

In this section, we state some more known results related to $H^1(G_K, J[2])$ where J is the Jacobian variety of a genus two curve defined by $y^2 = f(x)$ with f a polynomial of degree 6 defined over K. Most of the material in this section and more details can be found in [FTvL12, Section 2]. Also we assume K is a number field in this section, unless stated otherwise.

1.10.1 Homomorphism from $\text{Sel}^2(J)$ to $L^*/(L^*)^2K^*$

Let $L = K[x]/(f)$. We will describe a map $\text{Sel}^2(J) \to L^*/(L^*)^2K^*$ that we will use in several later parts of the thesis. We first give some useful notation. Let Ω denote the set of roots of f. Define $\bar{L} = L \otimes \bar{K}$. We get isomorphism $\bar{L} \cong \text{Map}(\Omega, \bar{K}) \cong \bar{K}^6$ where the first natural isomorphism is Galois equivariant and the second isomorphism is evaluation at the 6 roots in the fixed order $\omega_1, ..., \omega_6$. Via the first isomorphism, L is isomorphic to the set of Galois equivariant maps from Ω to $\bar{K}$, denoted by $\text{Map}_K(\Omega, \bar{K})$. We will be using these identifications in the discussion. The norm map N sends $\alpha \in \bar{L}$ to $\prod_{i=1}^{6} \alpha(\omega_i) \in \bar{K}$. It induces homomorphisms from $\mu_2(\bar{L})$ and $\mu_2(\bar{L})/\mu_2(\bar{K})$ to $\mu_2(\bar{K})$. For simplicity, we denote both of them as N and refer to as norms. Consider the the norm map $\mu_2(\bar{L}) \xrightarrow{N} \mu_2(\bar{K})$. Define $M \subset \mu_2(\bar{L})$ to be the kernel of this norm map N and we have the short exact sequence $0 \to M \to \mu_2(\bar{L}) \xrightarrow{N} \mu_2(\bar{K}) \to 0$. Let $\delta_i \in \bar{L}$ send ω_i to -1 and send ω_j to 1 for $i \neq j$. It can be checked that $\delta_i\delta_j$ form a basis for M as a $\mathbb{F}_2$-vector space. We also have a natural homomorphism $\beta : M \to J[2]$ that sends $\delta_i\delta_j$ to $\{(\omega_i, 0), (\omega_j, 0)\}$. This is a sujective homomorphism with kernel $\mu_2 =< \prod_{i=1}^{6} \delta_i >$ which gives a short exact sequence $0 \to \mu_2 \to M \to J[2] \to 0$. We let $-1 \in M$ denote the element $\prod_{i=1}^{6} \delta_i$ for simplicity.

It is known that $\mu : \mu_2(\bar{L}) \times \mu_2(\bar{L}) \to \mu_2$ that sends (f, g) to $(-1)^r$ where $r = \#\{\omega_i \in \Omega | f(\omega_i) = g(\omega_i) = -1\}$ is a perfect pairing. It can be checked that μ induces a well-defined natural perfect pairing $M \times \mu_2(\bar{L})/\mu_2(\bar{K}) \to \mu_2$. It can also be checked that this perfect pairing is compatible with the Weil pairing $e_2 : J[2] \times J[2]$ via the natural map $M \to J[2]$ defined above and the injection $\alpha : J[2] \to \mu_2(\bar{L})/\mu_2(\bar{K})$ that sends $\{(\omega_i, 0), (\omega_j, 0)\}$ to $\delta_i\delta_j$.

We get the following commutative diagram of the short exact sequences discussed above.

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & \mu_2(\bar{K}) & \xrightarrow{=} & \mu_2(\bar{K}) & & & & \\
 & & \downarrow & & \downarrow & & & & \\
1 & \longrightarrow & M & \longrightarrow & \mu_2(\bar{L}) & \xrightarrow{N} & \mu_2(\bar{K}) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \beta} & & \downarrow & & \downarrow{\scriptstyle =} & & \\
1 & \longrightarrow & J[2](\bar{K}) & \xrightarrow{\alpha} & \frac{\mu_2(\bar{L})}{\mu_2(\bar{K})} & \xrightarrow{N} & \mu_2(\bar{K}) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & & & \\
 & & 1 & & 1 & & & &
\end{array} \tag{1.10.1}$$

Via applying Hilbert's Theorem 90, we deduce the Kummer isomorphism $H^1(G_K, \mu_2(\bar{K})) \cong K^*/(K^*)^2$. By a generalized version of Hilbert's Theorem 90 [Ser79, Chapter X, Section 1 Exercise 2], which says $H^1(G_K, M^*) = 0$ for M a finite-dimensional unitary K-algebra, we have $H^1(G_K, \bar{L}^*) = 0$ and the Kummer isomorphism $H^1(G_K, \mu_2(\bar{L})) \cong L^*/(L^*)^2$. Therefore we have the following commutative diagram via taking the long exact sequneces of Galois cohomology.

$$\begin{array}{ccccccccc}
 & & & & K^*/(K^*)^2 & \xrightarrow{=} & K^*/(K^*)^2 & & \\
 & & & & \downarrow & & \downarrow & & \\
\mu_2(L) & \xrightarrow{N} & \mu_2(K) & \longrightarrow & H^1(G_K, M) & \longrightarrow & L^*/(L^*)^2 & \xrightarrow{N} & K^*/(K^*)^2 \\
\downarrow & & \downarrow{=} & & \downarrow{\scriptstyle \beta_*} & & \downarrow & & \downarrow{=} \\
H^0(G_K, \frac{\mu_2(\bar{L})}{\mu_2(\bar{K})}) & \xrightarrow{N} & \mu_2(K) & \longrightarrow & H^1(G_K, J[2]) & \xrightarrow{\alpha_*} & H^1(G_K, \frac{\mu_2(\bar{L})}{\mu_2(\bar{K})}) & \xrightarrow{N_*} & K^*/(K^*)^2 \\
 & & & & \downarrow{\scriptstyle \gamma} & & \downarrow & & \\
 & & & & \mathrm{Br}(K)[2] & \xrightarrow{=} & \mathrm{Br}(K)[2] & &
\end{array} , \tag{1.10.2}$$

where α_*, β_*, N_* are induced from α, β, N respectively.

We now quote some results whose proofs are in [FTvL12].

Proposition 1.10.1. [FTvL12, Proposition 2.2] *Assume that K is a number field or a local field. Then the composition of the map $\delta : J(K)/2J(K) \to H^1(G_K, J[2])$ defined in Section 1.9.1 with the map γ in the diagram above is zero.*

We denote the kernel of γ by $P^1(G_K, J[2])$. We know the image of $\delta : J(K)/2J(K) \to H^1(G_K, J[2])$ is contained in $\mathrm{Sel}^2(J)$. As discussed in [FTvL12, Remark 2.3], it follows from Proposition 1.10.1, applied to all K_v, and the fact that the natural map $\mathrm{Br}(K) \to \prod_v \mathrm{Br}(K_v)$ is injective, that $\mathrm{Sel}^2(J) \subset P^1(G_K, J[2])$.

From (1.10.2), the kernel of the homomorphism $H^1(G_K, \mu_2(\bar{L})/\mu_2(\bar{K})) \to \mathrm{Br}(K)[2]$ is isomorphic to the image of $L^*/(L^*)^2$ in $H^1(G_K, \mu_2(\bar{L})/\mu_2(\bar{K}))$ which is isomorphic to $L^*/(L^*)^2K^*$. This gives a homomorphism

$$\kappa : P^1(G_K, J[2]) \to L^*/(L^*)^2K^*,$$

induced by α_*, whose restriction gives a homomorphism $\mathrm{Sel}^2(J) \to L^*/(L^*)^2K^*$.

1.10.2 Fake Selmer

By Proposition 1.10.1, the following map is well-defined.

Definition 1.10.2. [FTvL12, Definition 2.4] The composition

$$\kappa \circ \delta : J(K)/2J(K) \to L^*/(L^*)^2K^*$$

is called the *Cassels map*.

Remark 1.10.3. We have explicit formula for the Cassels map:

$$[\{(u_1, v_1), (u_2, v_2)\}] \mapsto (x - u_1)(x - u_2),$$

in the case $v_1v_2 \neq 0$, see [FTvL12, Proposition 2.5]. The formula in the special cases can be found in [CF96, Chapter 6, Section 1]. In particular, when $(u_i, v_i) = (\omega, 0)$ is a K-rational Weierstrass point, we replace the ω-component of $(x - u_i) \in L \subset \bar{L} \cong \bar{K}^6$ by $-f'(\omega)$.

From (1.10.2), we have that $\ker \alpha_*$ equals the image of $\mu_2(K)$ in $H^1(G_K, J[2])$. This implies that $\ker \alpha_*$ has order 1 or 2. Since the image of $\mu_2(K)$ is contained in $\mathrm{Im}\, \beta_*$, it is contained in $P^1(G_K, J[2])$ and hence $\ker \alpha_* = \ker \kappa$. From [PS97, Lemma 9.1], we know $-1 \in \mu_2(K)$ is mapped to the element in $H^1(G_K, J[2])$ that is represented by the cocycle $(\sigma \mapsto \{(\omega, 0)^\sigma, (\omega, 0)\})$ for some fixed Weierstrass point $(\omega, 0)$. This implies by [PS99, Corollary 4] that $\ker \alpha_*$ is generated by the class of the principal homogeneous space $\mathrm{Pic}^1(\mathcal{C})$. [PS97, Lemma 11.2] gives a condition based on how f factors that tells whether or not $\ker \alpha_*$ is trivial. In particular, in the case where f has a rational root, then $\ker \alpha_*$ is trivial. Furthermore, when K is a local field, [PS99, Lemma 1] shows that $\ker \alpha_*$ is always trivial. Hence, when K is a number field, we have $\ker \alpha_* \subset \mathrm{Sel}^2(J)$ and $\ker \alpha_*$ measures the difference between $\mathrm{Sel}^2(J)$ and its image under κ in $L^*/(L^*)^2K^*$, which is known as the *fake Selmer group*, denoted

by $\mathrm{Sel}^2_{fake}(J)$.

Let Γ denote the subgroup of $L^* \times K^*$ that consist of all elements (δ, n) such that $N(\delta) = n^2$. Define the homomorphism $\chi : L^* \to \Gamma$ that sends ζ to $(\zeta^2, N(\zeta))$. We quote the following proposition and corollary with proofs in [FTvL12].

Proposition 1.10.4. [FTvL12, Proposition 2.6] *There is a unique isomorphism $\gamma : \Gamma/\operatorname{Im}\chi \to H^1(G_K, M)$ that sends the class of (δ, n) to the class of the cocycle $(\sigma \mapsto \sigma(\zeta)/\zeta)$, where $\zeta \in \bar{L}$ is any element satisfying $\zeta^2 = \delta$ and $N(\zeta) = n$. The composition of γ with the map $H^1(G_K, M) \to L^*/(L^*)^2$ sends (δ, n) to δ. The kernel $\ker\alpha_* = \ker\kappa$ is generated by the image of $(1, -1) \in \Gamma/\operatorname{Im}\chi$ under the composition of γ with the map $\beta_* : H^1(G_K, M) \to H^1(G_K, J[2])$.*

Corollary 1.10.5. [FTvL12, Corollary 2.9] *The composition of $\gamma : \Gamma/\operatorname{Im}\chi \to H^1(G_K, M)$ with the map $\beta_* : H^1(G_K, M) \to H^1(G_K, J[2])$ induces an isomorphism $\Gamma/(K^* \operatorname{Im}\chi) \to P^1(G_K, J[2])$. Note here we identify K^* with its image under the map $x \mapsto (x, x^3)$.*

We make the following remark to give notations for Selmer elements corresponding to the same fake Selmer element.

Remark 1.10.6. From the discussions above, we know that given a fake Selmer element in $L^*/(L^*)^2K^*$ represented by $\delta \in L^*$, the Selmer elements corresponding to it under the identification of $\Gamma/(K^* \operatorname{Im}\chi) \to P^1(G_K, J[2])$ in Corollary 1.10.5 are presented by (δ, n) and $(\delta, -n)$ where $N(\delta) = n^2$ by Proposition 1.10.4. From the previous discussion, we know that $\mathrm{Sel}^2(J) \cong \mathrm{Sel}^2_{fake}(J)$ in the case where f has a root defined over K. It can be shown that if f has a root defined over K, then $(1, -1) \in \operatorname{Im}\chi$ which indeed implies that (δ, n) and $(\delta, -n)$ represent the same Selmer element. Note that it is also compatible with Proposition 1.10.4 since $\ker\alpha_*$ measures the difference between $\mathrm{Sel}^2(J)$ and $\mathrm{Sel}^2_{fake}(J)$. In particular, in the case where f has a root defined over K, we have $P^1(G_K, J[2]) \cong \{\delta \in L^*/(L^*)^2K^* : N(\delta) \text{ is a square}\}$.

1.11 Explicit 2-Coverings of the Jacobian

In this section, we let J be the Jacobian variety of a genus two curve defined by $y^2 = f(x)$ with f a degree 6 polynomial defined over a number field K. Let Ω represent the set of 6 roots of f, denoted by $\omega_1, ..., \omega_6$. Recall in Proposition 1.5.10, we showed the isomorphism classes of 2-coverings of J are parameterized by $H^1(G_K, J[2])$. Also, in Section 1.10.1, we defined $P^1(G_K, J[2]) = \ker(H^1(G_K, J[2]) \xrightarrow{\gamma} \mathrm{Br}(K)[2])$ as in (1.10.2). In this section, we state the following theorem on the explicit 2-coverings of J corresponding

to elements in $P^1(G_K, J[2]) \subset H^1(G_K, J[2])$. As discussed in Section 1.10.1, we have $\mathrm{Sel}^2(J) \subset P^1(G_K, J[2])$ as K is a number field. This theorem is essential in the later chapters of the thesis. We note that this theorem in fact works over any field of characteristic different from 2.

Theorem 1.11.1. [FTvL12, Proposition 7.2, Theorem 7.4, Appendix B]*Let J be the Jacobian variety of a genus two curve defined by $y^2 = f(x)$ where f is a degree 6 polynomial and $\epsilon \in P^1(G_K, J[2])$. Embed J in $\mathbb{P}^{15}$ via the coordinates $k_{11}, k_{12}, ..., k_{44}, b_1, ..., b_6$. There exists $J_\epsilon \subset \mathbb{P}^{15}$ with Galois invariant coordinates $u_0, ..., u_9, v_1, ..., v_6$ and a linear isomorphism ϕ_ϵ such that J_ϵ is defined over K and $(J_\epsilon, [2] \circ \phi_\epsilon)$ is a 2-covering of J whose isomorphism class corresponds to the cocycle class ϵ. Moreover, ϕ_ϵ can be explicitly represented by the 16×16 matrix $R = \begin{bmatrix} R_1 & 0 \\ 0 & R_2 \end{bmatrix}$ for some 10×10 matrix R_1 and some 6×6 matrix R_2 given in the remark below.*

Remark 1.11.2. Since R is block diagonal, $u_0, ..., u_9$ are 10 even elements and $v_1, ..., v_6$ are 6 odd elements on J_ϵ. Here, the parity is corresponding to the induced involution ι_ϵ on J_ϵ as defined in Notation 1.6.4. We now give the explicit fomulae for R in the above theorem following the proof in [FTvL12]. Suppose $\epsilon \in P^1(G_K, J[2])$ is represented by (δ, n) for $\delta \in L^*$ with $N(\delta) = n^2$ as in Corollary 1.10.5. Define $\zeta \in \bar{L}$ such that $\zeta^2 = \delta$ and $N(\zeta) = n$. Let $I_1, ..., I_{10}$ be the 10 different subsets of Ω of size 3. Let T_1 be the diagonal matrix whose r^{th} diagonal entry is $\prod_{\omega \in I_r} \zeta(\omega) + \prod_{\omega \in \Omega \setminus I_r} \zeta(\omega)$ for $r = 1, ..., 10$. Since K is infinite, we can assume the entries of T_1 are nonzero by carefully picking ζ, δ and n representing ϵ. Let T_2 be the diagonal matrix whose r^{th} entry is $\zeta(\omega_r)$ for $r = 1, ..., 6$. Then define $S = \begin{bmatrix} 1 & 1 & ... & 1 \\ \omega_1 & \omega_2 & ... & \omega_6 \\ \vdots & \vdots & & \vdots \\ \omega_1^5 & \omega_2^5 & ... & \omega_6^5 \end{bmatrix}$. Let G be the matrix whose r^{th} row is

$$\frac{1}{4}\Big(\prod_{\omega \in I_r} \prod_{\psi \in \Omega \setminus I_r} (\psi - \omega)^{-1}\Big) \cdot (\lambda_{11}(I_r) \;\; \lambda_{12}(I_r) \;\; ... \;\; \lambda_{44}(I_r)),$$

with the explicit formulae of λ_{ij} in [FTvL12, Definition 6.11] which are defined over L_1, the splitting field of f. Then $R_1 = G^{-1} T_1 G$ and $R_2 = S T_2 S^{-1}$. We note the explicit formula for ϕ_ϵ is defined over $L_1(\sqrt{a_1}, ..., \sqrt{a_6})$ where $a_i = \delta(\omega_i)$. In fact, the formula for ϕ_ϵ given in Theorem 1.11.1 is a conjugation of the original construction given in [FTvL12, Proposition 7.2, Theorem 7.4] where the coordinates for $J, J_\epsilon \subset \mathbb{P}^{15}$ are given in [FTvL12, Definition 6.9, Definition 6.11] and the matrix representing the twist is $\begin{bmatrix} T_1 & 0 \\ 0 & T_2 \end{bmatrix}$. Note that this set of coordinates in general are not Galois invariant.

In this thesis, we will only be applying Theorem 1.11.1 in the case where $\epsilon \in \mathrm{Sel}^2(J)$. Consider $\epsilon \in \mathrm{Sel}^2(J)$. Theorem 1.11.1 gives an explicit formula for $\phi_\epsilon : J_\epsilon \subset \mathbb{P}^{15} \to J \subset \mathbb{P}^{15}$ such that $(J_\epsilon, [2] \circ \phi_\epsilon)$ the 2-covering of J corresponding to ϵ. In this thesis, we always embed J_ϵ in $\mathbb{P}^{15}$ via the Galois invariant coordinates $u_0, ..., u_9, v_1, ..., v_6$, unless stated otherwise.

Now suppose J_ϵ is embedded in $\mathbb{P}^{15}$ with any set of Galois invariant coordinates, denoted by $u'_0, ..., u'_9, v'_1..., v'_6$ where $u'_0, ..., u'_9$ are the even coordinates and the $v'_1, ..., v'_6$ are the odd basis with respect to the involution ι_ϵ. From Theorem 1.11.1 and Remark 1.11.2, under the coordinates $u'_0, ..., u'_9, v'_1..., v'_6$ and the standard coordinates for $J \subset \mathbb{P}^{15}$, we get that ϕ_ϵ is also represented by a block diagonal matrix that consists of a block of size 10 corresponding to the even coordinates and a block of size 6 corresponding to the odd coordinates. By Remark 1.3.3, we know that there are 72 defining equations of J_ϵ which are explicitly computable. In particular, the 72 defining equations consist of 30 odd quadratics where each monomial is a product of an even coordinate and an odd coordinate, 21 quadratics involving only the even coordinates and 21 quadratics in the form of $v'_i v'_j = Q_{ij,\epsilon}$, where $Q_{ij,\epsilon}$ is a quadratic in terms of the 10 even coordinates $u'_0, ..., u'_9$. Suppose the twisted Kummer surface $\mathcal{K}_\epsilon$ as in (1.6.2) has a K-rational point R, let $Q_1, Q_2 \in J_\epsilon$ be the two preimages of R, then $u'_i(Q_1) = u'_i(Q_2)$ for any i. Suppose $Q_1 \neq Q_2$, then $v'_i(Q_1) \neq 0$ for some i. Hence, let $a = Q_{ii,\epsilon}(u'_0(Q_1), ..., u'_9(Q_1))$, we get $a \in K$ and $K(Q_1) = K(Q_2) = K(\sqrt{a})$. Note since we can compute the explicit defining equations of J_ϵ, a is explicitly computable given the defining equation of $\mathcal{C}$, ϵ and the coordinates of R. Similarly, we can test if a local point on $\mathcal{K}_\epsilon(K_v)$ has a lift on $J_\epsilon(K_v)$ for any place v of K.

Remark 1.11.3. In the case where $Q_1 = Q_2$, which makes R a singular point on $\mathcal{K}_\epsilon$, Q_1, Q_2 are defined over K and we define a to be 1. So we always have $K(Q_1) = K(Q_2) = K(\sqrt{a})$ for a nonzero $a \in K$.

Chapter 2

The Cassels-Tate Pairing in the Case of a Richelot Isogeny

In this chapter, we will be studying the Cassels-Tate pairing for Jacobians of genus two curves that admit Richelot isogenies, which are a special type of isogenies defined in Section 2.1.1. We will end this chapter with a worked example which shows that carrying out a descent by Richelot isogeny and computing the Cassels-Tate pairing can achieve the same rank bound as obtained from a 2-descent calculation. In this chapter, unless otherwise stated, we assume K is a number field.

2.1 Definition of the Pairing

In this section, we give the definition of a Richelot isogeny. We then adapt the definition of the Cassels-Tate pairing in the case of a Richelot isogeny and show the compatibility of this new definition with the Weil pairing definition of the Cassels-Tate pairing given in Section 1.8.1.

2.1.1 Polarized isogeny and Richelot isogeny

We first give the definition of a polarized isogeny that is taken from [BD11, Definition 2.5].

Let (A, λ_A), (B, λ_B) be principally polarized abelian varieties of dimension d. We say that an isogeny $\phi : A \to B$ is a *polarized* $(n_1, n_2, ..., n_r)$*-isogeny* if $\ker \phi(\bar{K}) \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times ... \times \mathbb{Z}/n_r\mathbb{Z}$ and $\widehat{\phi} \circ \lambda_B \circ \phi = n\lambda_A$, where $\widehat{\phi}$ is the dual isogeny of ϕ and $n^d = \prod_{i=1}^{r} n_i$.

Richelot isogenies are the polarized $(2, 2)$-isogenies between Jacobians of genus 2 curves.

The following is discussed in [CF96, Chapter 9, Section 1]. Any finite subgroup on an abelian variety can be the kernel of an isogeny of abelian varieties. However, not all subgroups of order 4 can be the kernel of a Richelot isogeny. Consider (A, λ_A), a principally polarized abelian variety. Let $\phi : A \to B$ be

an isogeny with $\ker\phi \subset A[n]$. It is shown in [Mil86, Proposition 16.8] and [BD11, Lemma 2.4] that there exists a polarization $\lambda_B : B \to B^\vee$ such that $\widehat{\phi} \circ \lambda_B \circ \phi = n\lambda_A$ if and only if $\ker\phi$ is isotropic with respect to the Weil pairing e_n, which means e_n is trivial when restricted to $\ker\phi \times \ker\phi$. The above argument when $A = J$ and $n = 2$ describes Richelot isogenies. It can be checked that the kernel of a Richelot isogeny is actually a maximal isotropic subgroup of $J[2]$ with respect to e_2.

Let $\mathcal{C}$ be a genus two curve defined by $y^2 = f(x)$ whose Jacobian variety J admits a Richelot isogeny. By the discussion above and Lemma 1.7.6, we know the nontrivial elements in the kernel of the Richelot isogeny partition the 6 roots of $f(x)$ into 3 disjoint pairs in the case where f is degree 6. It is pointed out by Schaefer that there are interesting Richelot isogenies where the kernel is defined over K as a whole but the elements are not. However, in this thesis, we assume all points in the kernel are defined over K as it is also assumed in [CF96, Chapter 9]. We have the following proposition from [CF96, Chapter 9 Section 2] and [Fly18, Section 3].

Proposition 2.1.1. *Suppose the curve $\mathcal{C}$ is of the form*

$$\mathcal{C} : y^2 = f(x) = G_1(x)G_2(x)G_3(x),$$

where $G_j(x) = g_{j2}x^2 + g_{j1}x + g_{j0}$, and each $g_{ji} \in K$. Then there is a Richelot isogeny ϕ from J, the Jacobian of $\mathcal{C}$, to $\widehat{J}$, the Jacobian of the following genus two curve:

$$\widehat{\mathcal{C}} : \triangle y^2 = L_1(x)L_2(x)L_3(x),$$

where each $L_i(x) = G_j'(x)G_k(x) - G_j(x)G_k'(x)$, for $[i,j,k] = [1,2,3], [2,3,1], [3,1,2]$, and $\triangle = \det(g_{ij})$ which we assume to be non-zero.

In addition, the kernel of ϕ consists of the identity $\mathcal{O}_J$ and the 3 divisors of order 2 given by $G_i = 0$. We have the similar result for the dual isogeny $\widehat{\phi}$.

Moreover, any genus two curve $\mathcal{C}$ that admits a Richelot isogeny with all the elements of the kernel K-rational is of the form $y^2 = f(x) = G_1(x)G_2(x)G_3(x)$ as above.

Remark 2.1.2. We exclude the case $\triangle = 0$ in the above proposition. In fact, by [CF96, Chapter 14], $\triangle = 0$ implies that the Jacobian of $\mathcal{C}$ is the product of elliptic curves. Also, it can be checked that the analogue of $\triangle$ for $\widehat{C}$ is $2\triangle^2$, so no need to have further condition like $\triangle \neq 0$ from $\widehat{C}$. Lastly, in the case where G_i is linear, say $G_i = a(x - b)$, then we say $\{(b, 0), \infty\}$ is the divisor given by $G_i = 0$ which gives an element in $\ker\phi$.

We use the notation in Proposition 2.1.1 and denote the nontrivial elements in the kernel of ϕ by P_i corresponding to the divisors of order 2 given by

$G_i = 0$ as well as denote the nontrivial elements in the kernel of $\widehat{\phi}$ by P_i'. From [CF96, Chapter 9, Section 2] and [TY09, Section 3.2], we have the following description of the Richelot isogeny ϕ. Associated with a Weierstrass point $P = (\omega_1, 0)$ with $G_1(\omega_1) = 0$, $\phi : J \to \widehat{J}$ is given explicitly as

$$\{(x, y), P\} \mapsto \{(z_1, t_1), (z_2, t_2)\},$$

where z_1, z_2 satisfy

$$G_2(x)L_2(z) + G_3(x)L_3(z) = 0;$$

and (z_i, t_i) satisfies

$$yt_i = G_2(x)L_2(z_i)(x - z_i).$$

Denote the set of two points on $\mathcal{C}$ given by $G_i = 0$ by S_i for $i = 1, 2, 3$. From the explicit description above, we know that the preimages of P_1' under ϕ are precisely $\{\{Q_1, Q_2\} \in J[2] \text{ such that } Q_1 \in S_2, Q_2 \in S_3\}$. Similarly we know the preimages of P_2' and P_3'.

2.1.2 The Weil pairing for Richelot isogeny

Let (J, λ_1) and $(\widehat{J}, \lambda_2)$ be Jacobian varieties of genus two curves defined over a field K with characteristic not equal to 2. Assume there is a Richelot isogeny $\phi : J \to \widehat{J}$ with $\widehat{\phi}$ being its dual, i.e. $\phi \circ \widehat{\phi} = [2]$. Then we have the Weil pairing

$$e_\phi : J[\phi] \times \widehat{J}[\widehat{\phi}] \to \bar{K}^*,$$

such that $e_\phi(P, Q) = e_{2,J}(P, Q')$ for any $Q' \in J[2]$ such that $\phi(Q') = Q$. Note that the image of e_ϕ is $\mu_2(\bar{K}^*) \subset \bar{K}^*$. Recall $\ker \phi$ is isotropic with respect to $e_{2,J}$, as discussed in Section 2.1.1. This implies that $e_{2,J}(P, Q') = e_{2,J}(P, Q'')$ if $\phi(Q') = \phi(Q'')$ and hence e_ϕ is well-defined. This implies that $e_\phi(P_i, P_i') = 1$ for any $i = 1, 2, 3$ and $e_\phi(P_i, P_j') = -1$ for any $i \neq j$ by Lemma 1.7.6 and the discussion at the end of Section 2.1.1. Note, in this chapter, we denote $e_{2,J}$ to be the e_2 Weil pairing for the Jacobian variety J, and similarly we have $e_{2,\widehat{J}}$.

We make the following remarks on some useful notations and properties related to the Weil pairing that are needed later.

Remark 2.1.3.

(i) We let $\cup_\phi : C^1(G_K, J[\phi]) \times C^1(G_K, \widehat{J}[\widehat{\phi}]) \to C^2(G_K, \bar{K}^*)$ be the cup-product pairing associated to e_ϕ. Similarly we have $\cup_{2,J}$ and $\cup_{2,\widehat{J}}$. In the case where K is a global field, we also have $\cup_{\phi,v}, \cup_{2,J,v}$ and $\cup_{2,\widehat{J},v}$ defined similarly as in Remark 1.7.4(iii). Similar to Remark 1.7.4(i), we sometimes let $\cup_\phi$ denote the cup product $H^1(G_K, J[\phi]) \times H^1(G_K, \widehat{J}[\widehat{\phi}]) \to H^2(G_K, \bar{K}^*)$.

(ii) Since $e_\phi(P, \phi(Q)) = e_{2,J}(P, Q)$ for any $P \in J[\phi], Q \in J[2]$, we have $a \cup_\phi \phi(b) = a \cup_{2,J} b$ for any $a \in C^1(G_K, J[\phi]), b \in C^1(G_K, J[2])$.

(iii) Given any $P \in J[2], Q \in \widehat{J}[2]$, we know $e_{2,J}(P, \widehat{\phi}(Q)) = e_{2,\widehat{J}}(\phi(P), Q)$ by [Mil08, Proposition 13.2(a)], which implies that $e_\phi(P, Q) = e_{\widehat{\phi}}(Q, P)$ for any $P \in J[\phi], Q \in \widehat{J}[\widehat{\phi}]$. This further implies $e_{2,J}(P, Q) = e_{\widehat{\phi}}(\phi(P), Q)$ for $P \in J[2]$ and $Q \in J[\phi]$. Hence, we have $a \cup_{2,J} \widehat{\phi}(b) = \phi(a) \cup_{2,\widehat{J}} b$ for any $a \in C^1(G_K, J[2]), b \in C^1(G_K, \widehat{J}[2])$. We also have $a \cup_{2,J} b = \phi(a) \cup_{\widehat{\phi}} b$, for any $a \in C^1(G_K, J[2]), b \in C^1(G_K, J[\phi])$.

2.1.3 The Cassels-Tate pairing on $\text{Sel}^\phi(J)$

Let (J, λ_1) and $(\widehat{J}, \lambda_2)$ be Jacobian varieties of genus two curves defined over a number field K such that there exists a Richelot isogeny $\phi : J \to \widehat{J}$ with $\widehat{\phi} : \widehat{J} \to J$ being its dual isogeny. We will now define a pairing $\langle a, a' \rangle$ for $a, a' \in \text{Sel}^\phi(J)$ and show that this is compatible with the Weil pairing definition of $\langle\ ,\ \rangle_{CT}$ defined on $Ш(J)[\phi] \subset Ш(J)[2]$ as in Section 1.8.1. We first note the following lemma.

Lemma 2.1.4. *Let (J, λ_1) and $(\widehat{J}, \lambda_2)$ be Jacobian varieties of genus two curves such that there exists a Richelot isogeny $\phi : J \to \widehat{J}$ with $\widehat{\phi} : \widehat{J} \to J$ being its dual isogeny. We have the following:*

(i) The map $H^2(G_K, J[\phi]) \xrightarrow{res} \prod_v H^2(G_{K_v}, J[\phi])$ is injective.

(ii) For any $b \in Sel^\phi(J)$, there exists $b_1 \in H^1(G_K, \widehat{J}[2])$ mapping to b.

Proof. Recall we assume all points in $J[\phi]$ are over K. The proof is almost identical to the proof of Lemma 1.8.6(i) and therefore omitted. The proof of (ii) from (i) is again almost identical to the proof of Lemma 1.8.6(ii) and therefore also omitted.

□

Remark 2.1.5. Note that from [Cas62, Lemma 5.1], we have the injectivity of $H^2(G_K, A) \xrightarrow{res} \prod_v H^2(G_{K_v}, A)$ when A is a G_K-module that is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ when considered only as a $\mathbb{Z}$-module. Hence, without assuming all points in $J[\phi]$ are defined over K, (i) still holds and so (ii) also holds in Lemma 2.1.4.

The definition of the pairing $\langle\ ,\ \rangle$

Let $a, a' \in \mathrm{Sel}^{\phi}(J)$. From the lemma above, we know that there is always a global lift $a_1 \in H^1(G_K, \widehat{J}[2])$ for $a \in \mathrm{Sel}^{\phi}(J) \subset H^1(G_K, J[\phi])$ induced by the map $\widehat{J}[2] \xrightarrow{\widehat{\phi}} J[\phi]$.

Similar to the diagram in Proposition 1.8.5, we have the commutative diagram below.

$$\begin{array}{ccccc}
\widehat{J}(K_v) & \xrightarrow[\widehat{\phi}]{} & J(K_v) & \xrightarrow{\delta_{\widehat{\phi}}} & H^1(G_{K_v}, \widehat{J}[\widehat{\phi}]) \\
{\scriptstyle =}\downarrow & & {\scriptstyle \phi}\downarrow & & {\scriptstyle \iota}\downarrow{\scriptstyle \rho_v \mapsto \delta_2(P_v) - a_{1,v}} \\
\widehat{J}(K_v) & \xrightarrow[2]{} & \widehat{J}(K_v) & \xrightarrow{\delta_2} & H^1(G_{K_v}, \widehat{J}[2]) \\
{\scriptstyle \widehat{\phi}}\downarrow & & {\scriptstyle =}\downarrow & & {\scriptstyle \widehat{\phi}}\downarrow{\scriptstyle \delta_2(P_v) \mapsto a_v \quad a_{1,v} \mapsto a_v} \\
J(K_v) & \xrightarrow[\phi]{} & \widehat{J}(K_v) & \xrightarrow[\delta_{\phi}]{P_v \mapsto a_v} & H^1(G_{K_v}, J[\phi])
\end{array}$$

Let v be a place of K. Let $P_v \in \widehat{J}(K_v)$ be the lift of $a_v \in H^1(G_{K_v}, J[\phi])$, then $\delta_2(P_v)$ and $a_{1,v}$ in $H^1(G_{K_v}, \widehat{J}[2])$ both map to a_v. Hence, let $\rho_v \in H^1(G_{K_v}, \widehat{J}[\widehat{\phi}])$ denote a lift of $\delta_2(P_v) - a_{1,v}$ and define $\eta_v = \rho_v \cup_{\widehat{\phi},v} a'_v \in H^2(G_{K_v}, \bar{K_v}^*)$. Here $\cup_{\widehat{\phi},v}$ denotes the cup product $H^1(G_{K_v}, \widehat{J}[\widehat{\phi}]) \times H^1(G_{K_v}, J[\phi]) \to H^2(G_{K_v}, \bar{K}^*)$ associated to $e_{\widehat{\phi}}$. We define

$$\langle a, a' \rangle := \sum_v \mathrm{inv}_v(\eta_v).$$

We sometimes refer to $\mathrm{inv}_v(\eta_v)$ above as the local Cassels-Tate pairing between $a, a' \in \mathrm{Sel}^{\phi}(J)$ for a place v of K.

Proposition 2.1.6. *Let (J, λ_1) and $(\widehat{J}, \lambda_2)$ be Jacobian varieties of genus two curves such that there exists a Richelot isogeny $\phi : J \to \widehat{J}$ with $\widehat{\phi} : \widehat{J} \to J$ being its dual isogeny. For $a, a' \in Sel^{\phi}(J)$,*

$$\langle a, a' \rangle = \langle \psi(a), \psi(a') \rangle_{CT},$$

where $\langle\ ,\ \rangle$ is defined above and $\psi : Sel^{\phi}(J) \to Sel^{2}(J)$ is the restriction of the natural map $H^1(G_K, J[\phi]) \to H^1(G_K, J[2])$ induced from the inclusion $J[\phi] \to J[2]$.

Proof. From Lemma 2.1.4, we know that there exists $a_1 \in H^1(G_K, \widehat{J}[2])$ represented by $s_1 \in Z^1(G_K, \widehat{J}[2])$ such that $\widehat{\phi}(s_1) = t \in Z^1(G_K, J[\phi])$ representing a. Also let $t' \in Z^1(G_K, J[\phi])$ represent a' such that there exists $s'_1 \in Z^1(G_K, \widehat{J}[2])$ with $\widehat{\phi}(s'_1) = t'$.

Let $s \in C^1(G_K, J[4])$ with $\phi(s) = s_1$. Treating t in $Z^1(G_K, J[2])$, we have t representing $\psi(a)$ and $2s = \widehat{\phi}(s_1) = t$. Similarly, treating t' in $Z^1(G_K, J[2])$, we have t' representing $\psi(a')$. Let $\cup_{2,J} : C^1(G_K, J[2]) \times C^1(G_K, J[2]) \to$

$C^2(G_K, \bar{K}^*)$ denote the cup-product pairing associated to $e_{2,J}$. Then $ds \cup_{2,J} t' = ds \cup_{2,J} \hat{\phi}(s_1') = \phi(ds) \cup_{2,\widehat{J}} s_1' = ds_1 \cup_{2,\widehat{J}} s_1'$ by Remark 2.1.3(iii), where $\cup_{2,\widehat{J}} : C^1(G_K, \widehat{J}[2]) \times C^1(G_K, \widehat{J}[2]) \to C^2(G_K, \bar{K}^*)$ denotes the cup product pairing associated to $e_{2,\widehat{J}}$. This implies that $ds \cup_{2,J} t' = 0$ as s_1 is a cocycle. Hence following the Weil pairing definition of $\langle \psi(a), \psi(a') \rangle_{CT}$, we can pick $r = 0$.

Let v be a place of K. Let $P_v \in \widehat{J}(K_v)$ be a lift of a_v. There exists $Q_v \in \widehat{J}(\bar{K}_v)$ such that $2Q_v = P_v$ and $d\widehat{\phi}(Q_v)$ is equal to the image of t_v in $Z^1(G_{K_v}, J)$. Now dQ_v, as a cocycle in $Z^1(G_K, \widehat{J}[2])$, represents $\delta_2(P_v)$. By Remark 1.7.4(i), we need to compute $(dQ_v - s_{1,v} + d\gamma) \cup_{\widehat{\phi},v} t_v'$ for some $\gamma \in \widehat{J}[2]$ following the definition of $\langle a, a' \rangle$. Note here $\cup_{\widehat{\phi},v}$ denoted the cup product $C^1(G_{K_v}, \widehat{J}[\widehat{\phi}]) \times C^1(G_{K_v}, J[\phi]) \to C^2(G_{K_v}, \bar{K}^*)$ associated to $e_{\widehat{\phi}}$.

Now let $R_v \in \widehat{J}(\bar{K}_v)$ such that $2R_v = Q_v$, we have that $d(2\widehat{\phi}(R_v)) = d(\widehat{\phi}(Q_v))$ is equal to the image of t_v in $Z^1(G_{K_v}, J)$. Following the definition of $\langle \psi(a), \psi(a') \rangle_{CT}$, we need to compute $d(\widehat{\phi}(R_v) - s_v) \cup_{2,J,v} t_v' \in C^2(G_{K_v}, \bar{K_v}^*)$.

Hence, it suffices to show that $(dQ_v + d\gamma - s_{1,v}) \cup_{\widehat{\phi},v} t_v'$ and $d(\widehat{\phi}(R_v) - s_v) \cup_{2,J,v} t_v'$ represent the same element in $H^2(G_{K_v}, \bar{K_v}^*)$, where γ is any element in $\widehat{J}[2]$ such that $(dQ_v + d\gamma - s_{1,v}) \cup_{\widehat{\phi},v} t_v'$ is well-defined. By Remark 2.1.3(iii), $(dQ_v + d\gamma - s_{1,v}) \cup_{\widehat{\phi},v} t_v' = (d\widehat{\phi}(R_v) + d\theta - s_v) \cup_{2,J,v} t_v'$, where $\theta \in J[4]$ such that $\phi(\theta) = \gamma$. Hence, it suffices to show that $d\theta \cup_{2,J,v} t_v'$ represents the trivial element in $H^2(G_{K_v}, \bar{K_v}^*)$. But $d\theta \cup_{2,J,v} t_v' = d\theta \cup_{2,J,v} \widehat{\phi}(s_{1,v}') = d\gamma \cup_{2,\widehat{J},v} s_{1,v}'$ by Remark 2.1.3(iii). Recall $\gamma \in \widehat{J}[2]$, hence we are done.

□

Remark 2.1.7. Proposition 2.1.6 shows that $\langle\ ,\ \rangle$ is compatible with $\langle\ ,\ \rangle_{CT}$. So we will refer to this as the Cassels-Tate pairing on $\text{Sel}^{\phi}(J) \times \text{Sel}^{\phi}(J)$, also denoted as $\langle\ ,\ \rangle_{CT}$. Note that this compatibility also shows that this definition is independent of all the choices we make by Proposition 1.8.4.

2.2 Explicit Embeddings and Maps

In this section, we will give some explicit embeddings and maps. These will become useful in the explicit computation for the Cassels-Tate pairing in the case of Richelot isogenies. For the remaining of this chapter, we will be working with Jacobian variety J of a genus two curve defined over a number field K where all points in $J[2]$ are defined over K, for simplicity. Furthermore we assume there exists a Richelot isogeny $\phi : J \to \widehat{J}$ with its dual $\widehat{\phi}$. Note that this implies all points in $\widehat{J}[\widehat{\phi}]$ are defined over K by Proposition 2.1.1.

Since we assume points in $J[2]$ are all defined over K, we can reduce the defining polynomial of the curve $\mathcal{C}$, $y^2 = f(x)$, such that f is degree 5. By

Proposition 2.1.1, we always assume the following throughout the remaining of this chapter.

Our genus two curve is of the form:

$$C : y^2 = f(x) = G_1(x)G_2(x)G_3(x),$$

where $G_1(x) = \lambda(x - \omega_1); G_2(x) = (x - \omega_2)(x - \omega_3); G_3(x) = (x - \omega_4)(x - \omega_5)$ with $\lambda, \omega_i \in K$ and $\lambda \neq 0$.

The Richelot isogeny ϕ from J, the Jacobian of $\mathcal{C}$, to $\widehat{J}$, the Jacobian of the following curve, as in Proposition 2.1.1.

$$\widehat{\mathcal{C}} : \triangle y^2 = L_1(x)L_2(x)L_3(x).$$

Recall, we denote the nontrivial elements in $J[\phi]$ by P_1, P_2, P_3 where P_i corresponds to the divisor given by $G_i = 0$ and the nontrivial elements in $\widehat{J}[\widehat{\phi}]$ by P_1', P_2', P_3' where P_i' corresponds to the divisor given by $L_i = 0$ as in Proposition 2.1.1.

2.2.1 Explicit embeddings

In this section, we describe some well-known embeddings that are useful in the explicit computation.

Embbedings of $\mathbf{H^1(G_K, J[\phi])}$ and $\mathbf{H^1(G_K, J[2])}$

Recall all points in $J[2]$ and $\widehat{J}[\widehat{\phi}]$ are defined over K. From the exact sequence below

$$0 \to J[\phi] \xrightarrow{w_\phi} (\mu_2)^3 \xrightarrow{N} \mu_2 \to 0,$$

where $w_\phi : P \mapsto (e_\phi(P, P_1'), e_\phi(P, P_2'), e_\phi(P, P_3'))$ and $N : (a, b, c) \mapsto abc$, we then get

$$H^1(G_K, J[\phi]) \xrightarrow{inj} H^1(G_K, (\mu_2)^3) \cong (K^*/(K^*)^2)^3 \xrightarrow{N_*} H^1(G_K, \mu_2) \cong K^*/(K^*)^2,$$

where $\cong$ denotes the Kummer isomorphism derived from Hilbert's Theorem 90 and N_* is induced by N. Note that the induced $H^1(G_K, J[\phi]) \to H^1(G_K, (\mu_2)^3)$ is injective as the map $(\mu_2)^3 \xrightarrow{N} \mu_2$ is surjective. Furthermore, the image of this injection contains precisely all the elements with norm a square by the exactness of the sequence above. We have a similar embedding for $H^1(G_K, \widehat{J}[\widehat{\phi}])$.

Also, from the exact sequence below

$$0 \to J[2] \xrightarrow{w_2} (\mu_2)^5 \xrightarrow{N} \mu_2 \to 0,$$

where $w_2 : P \mapsto (e_2(P, \{(\omega_1, 0), \infty\}), ..., e_2(P, \{(\omega_5, 0), \infty\}))$ and $N : (a, b, c, d, e) \mapsto abcde$, we then get

$$H^1(G_K, J[2]) \xrightarrow{inj} H^1(G_K, (\mu_2)^5) \cong (K^*/(K^*)^2)^5 \xrightarrow{N_*} H^1(G_K, \mu_2) \cong K^*/(K^*)^2,$$

where $\cong$ denotes the Kummer isomorphism derived from Hilbert's Theorem 90 and N_* is induced by N. Again the induced $H^1(G_K, J[2]) \to H^1(G_K, (\mu_2)^5)$ is injective as the map $(\mu_2)^5 \xrightarrow{N} \mu_2$ is surjective. Furthermore, the image of this injection also contains precisely all the elements with norm a square from the exact sequence above. In particular, we have

$$H^1(G_K, J[2]) \cong (K^*/(K^*)^2)^4.$$

Embedding of $\widehat{\mathbf{J}}(\mathbf{K})/\phi(\mathbf{J}(\mathbf{K}))$ and $\mathbf{J}(\mathbf{K})/\mathbf{2J}(\mathbf{K})$

General results show that we have the injection, which is the composition of the connecting map $\delta_\phi : \widehat{J}(K)/\phi(J(K)) \to H^1(G_K, J[\phi])$ and the embedding described above $H^1(G_K, J[\phi]) \to (K^*/(K^*)^2)^3$. This is discussed in [Fly18, Section 3] [CF96, Chapter 10 Section 2]. More explicitly, we have

$$\begin{array}{rccc} \mu^\phi : & \widehat{J}(K)/\phi(J(K)) & \longrightarrow & K^*/(K^*)^2 \times K^*/(K^*)^2 \times K^*/(K^*)^2 \\ & \{(x_1, y_1), (x_2, y_2)\} & \longmapsto & (L_1(x_1)L_1(x_2), L_2(x_1)L_2(x_2), L_3(x_1)L_3(x_2)) \end{array}.$$

Similarly we have the injection:

$$\begin{array}{rccc} \mu^{\widehat{\phi}} : & J(K)/\widehat{\phi}(\widehat{J}(K)) & \longrightarrow & K^*/(K^*)^2 \times K^*/(K^*)^2 \times K^*/(K^*)^2 \\ & \{(x_1, y_1), (x_2, y_2)\} & \longmapsto & (G_1(x_1)G_1(x_2), G_2(x_1)G_2(x_2), G_3(x_1)G_3(x_2)) \end{array}.$$

Note the following special cases. When x_j is a root of G_i, then $G_i(x_j)$ should be taken to be $\prod_{l \in \{1,2,3\} \setminus \{i\}} G_l(x_j)$. We have a similar solution when x_j is a root of L_i, which is replacing $L_i(x_j)$ with $\triangle \prod_{l \in \{1,2,3\} \setminus \{i\}} L_l(x_j)$. When $(x_j, y_j) = \infty$, then $G_i(x_j)$ is taken to be 1. In the case where one of L_i is linear and $(x_j, y_j) = \infty$, then $L_i(x_j)$ is taken to be 1.

On the other hand, we have a standard injection, which is the composition of the connecting map $\delta_2 : J(K)/2J(k) \to H^1(G_K, J[2])$ and the embedding described above $H^1(G_K, J[2]) \to (K^*/(K^*)^2)^5$. This can also be found in [Fly18, Section 3] [CF96, Chapter 10 Section 2].

$$\begin{array}{rccc} \mu : & J(K)/2J(K) & \longrightarrow & (K^*/(K^*)^2)^5 \\ & \{(x_1, y_1), (x_2, y_2)\} & \longmapsto & ((x_1 - \omega_1)(x_2 - \omega_1), ..., (x_1 - \omega_5)(x_2 - \omega_5)) \end{array}.$$

Note the following special cases. When $(x_j, y_j) = (\omega_i, 0)$, then $x_j - \omega_i$ should be taken to be $\lambda \prod_{l \in 1,2,3,4,5 \setminus \{i\}} (\omega_i - \omega_l)$. When $(x_j, y_j) = \infty$, then $x_j - \omega_i$ is taken to be λ.

Observe that the image of the maps μ^{ϕ} and $\mu^{\widehat{\phi}}$ are both contained in the kernel of $(K^*/(K^*)^2)^3 \xrightarrow{N} K^*/(K^*)^2$. Similarly, the image of μ is contained in the kernel of $(K^*/(K^*)^2)^5 \xrightarrow{N} K^*/(K^*)^2$.

2.2.2 Explicit maps

Using the embeddings described in Section 2.2.1, we can now prove the three propositions on explicit maps.

Proposition 2.2.1. *Under the embeddings of $H^1(G_K, J[\phi])$ and $H^1(G_K, \widehat{J}[\widehat{\phi}])$ in $(K^*/(K^*)^2)^3$ as described in Section 2.2.1, we get that the cup product $\cup_\phi$ induced by e_ϕ is*

$$H^1(G_K, J[\phi]) \times H^1(G_K, \widehat{J}[\widehat{\phi}]) \to Br(K)[2]$$

$$((a_1, b_1, c_1), (a_2, b_2, c_2)) \mapsto (a_1, a_2) + (b_1, b_2) + (c_1, c_2),$$

where $(\ ,\ )$ represents the quaternion algebra and here it also represents its equivalence class in $Br(K)[2]$ for simplicity.

Proof. Recall that the embedding $J[\phi] \to (\mu_2)^3$ is given by sending $P \in J[\phi]$ to $(e_\phi(P, P_1'), e_\phi(P, P_2'), e_\phi(P, P_3'))$ and the embedding $\widehat{J}[\widehat{\phi}] \to (\mu_2)^3$ is given by sending $Q \in \widehat{J}[\widehat{\phi}]$ to $(e_\phi(P_1, Q), e_\phi(P_2, Q), e_\phi(P_3, Q))$.

It can be checked that we have the following commutative diagram:

$$\begin{array}{ccc} J[\phi] \times \widehat{J}[\widehat{\phi}] & \xrightarrow{inj} & (\mu_2)^3 \times (\mu_2)^3 \\ \Big\downarrow{\scriptstyle e_\phi} & & \Big\downarrow{\scriptstyle f} \\ \mu_2 & \xrightarrow{\quad = \quad} & \mu_2, \end{array}$$

where f sends $((-1)^a, (-1)^b, (-1)^c), ((-1)^{a'}, (-1)^{b'}, (-1)^{c'})$ to $(-1)^{aa'+bb'+cc'}$ with $a, b, c \in \{0, 1\}$.

Therefore, by Remark 1.4.16, we get that the induced cup product is

$$H^1(K, J[\phi]) \times H^1(K, \widehat{J}(\widehat{\phi})) \to \mathrm{Br}(K)[2]$$

$$((a_1, b_1, c_1), (a_2, b_2, c_2)) \mapsto (a_1, a_2) + (b_1, b_2) + (c_1, c_2),$$

here $(\ ,\ )$ represents the the equivalence class of a quaternion algebra in $\mathrm{Br}(K)[2]$.

□

Proposition 2.2.2. *Under the embedding of $H^1(G_K, J[\phi])$ in $(K^*/(K^*)^2)^3$ and the embedding of $H^1(G_K, J[2])$ in $(K^*/(K^*)^2)^5$ as described in Section 2.2.1, the map $\Psi : H^1(G_K, J[\phi]) \to H^1(G_K, J[2])$ induced from the inclusion $J[\phi] \to J[2]$ is given by*

$$(a, b, c) \mapsto (1, c, c, b, b).$$

Proof. Recall the embedding of $H^1(G_K, J[2])$ in $(K^*/(K^*)^2)^5$, and the embedding of $H^1(G_K, J[\phi])$ in $(K^*/(K^*)^2)^3$ are induced from the short exact sequences with the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J[\phi] & \xrightarrow{w_\phi} & (\mu_2)^3 & \xrightarrow{N} & \mu_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle inc} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle =} & & \\ 0 & \longrightarrow & J[2] & \xrightarrow{w_2} & (\mu_2)^5 & \xrightarrow{N} & \mu_2 & \longrightarrow & 0. \end{array}$$

Suppose $P \in J[\phi]$ maps to (α, β, γ) via w_ϕ. Then $e_\phi(P, P_1') = \alpha, e_\phi(P, P_2') = \beta, e_\phi(P, P_3') = \gamma$. By definition, $e_\phi(P, \phi(Q)) = e_2(P, Q)$ for any $Q \in J[2]$. From the explicit description of ϕ in Section 2.1.1, we know $\alpha = e_2(P, \{(\omega_2, 0), (\omega_4, 0)\})$, $\beta = e_2(P, \{(\omega_1, 0), (\omega_5, 0)\})$ and $\gamma = e_2(P, \{\infty, (\omega_3, 0)\})$. Recall that $J[\phi]$ is isotropic with respect to e_2. This implies that $w_2(P) = (1, \gamma, \gamma, \beta, \beta)$. Therefore, we define $\psi(\alpha, \beta, \gamma) = (1, \gamma, \gamma, \beta, \beta)$, which makes the above diagram commute.

Now consider $\Psi : H^1(G_K, J[\phi]) \to H^1(G_K, J[2])$ which, via the embedding in Section 2.2.1, is the the natural restriction of $H^1(G_K, (\mu_2)^3) \to H^1(G_K, (\mu_2)^5)$ induced by ψ. It can be checked that $\Psi(a, b, c) = (1, c, c, b, b)$.

□

Proposition 2.2.3. *Under the embedding of $H^1(G_K, \widehat{J}[\widehat{\phi}])$ in $(K^*/(K^*)^2)^3$ and the embedding of $H^1(G_K, J[2])$ in $(K^*/(K^*)^2)^3$ as described in Section 2.2.1, the map $\Psi : H^1(G_K, J[2]) \to H^1(G_K, \widehat{J}[\widehat{\phi}])$ induced from $J[2] \xrightarrow{\phi} \widehat{J}(\widehat{\phi})$ is given by*

$$(a_1, a_2, a_3, a_4, a_5) \mapsto (a_1, a_2a_3, a_4a_5).$$

Proof. Consider the following commutative diagram of the exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J[2] & \xrightarrow{w_2} & (\mu_2)^5 & \xrightarrow{N} & \mu_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle =} & & \\ 0 & \longrightarrow & \widehat{J}[\widehat{\phi}] & \xrightarrow{w_{\widehat{\phi}}} & (\mu_2)^3 & \xrightarrow{N} & \mu_2 & \longrightarrow & 0. \end{array}$$

Suppose $P \in J[2]$ maps to $(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$ via w_2. Then we know $\alpha_i = e_2(P, \{(\omega_i, 0), \infty\})$. Recall $e_{\widehat{\phi}}(\phi(P), P_i) = e_2(P, P_i)$ by Remark 2.1.3(iii). This implies that $\phi(P)$ maps to $(\alpha_1, \alpha_2\alpha_3, \alpha_4\alpha_5)$ via $w_{\widehat{\phi}}$. Therefore, we can verify that the induced map $\Psi : H^1(G_K, J[2]) \to H^1(G_K, \widehat{J}[\widehat{\phi}])$ under the embeddings in Section 2.2.1 is given by

$$(a_1, a_2, a_3, a_4, a_5) \mapsto (a_1, a_2a_3, a_4a_5).$$

Remark 2.2.4. We observe that, under the assumption of this section, we have the following short exact sequence:

$$0 \to H^1(G_K, J[\phi]) \to H^1(G_K, J[2]) \to H^1(G_K, \widehat{J}[\widehat{\phi}]) \to 0.$$

The injectivity of the map $H^1(G_K, J[\phi]) \to H^1(G_K, J[2])$ is due to the surjectivity of $J(K)[2] \xrightarrow{\phi} \widehat{J}(K)[\widehat{\phi}]$. Observe that the element in $H^1(G_K, \widehat{J}[\widehat{\phi}])$ represented by (a, b, c) has a preimage in $H^1(G_K, J[2])$ represented by $(a, 1, b, 1, c)$ by Proposition 2.2.3. This implies that $H^1(G_K, J[2]) \to H^1(G_K, \widehat{J}[\widehat{\phi}])$ is surjective.

Remark 2.2.5. Let v be a place of K. We also have the explicit embeddings of $H^1(G_K, J[\phi])$ and $H^1(G_K, J[2])$ described in Section 2.2.1 as well as the explicit maps given in this section if we replace K with K_v or K_v^{nr}.

□

2.3 Prime Bound and Worked Example

Using the 3 propositions from Section 2.2.2, we can now explicitly compute the Cassels-Tate pairing in the case of a Richelot isogeny. More explicitly, for a Richelot isogeny between Jacobian varieties of genus two curves $\phi : J \to \widehat{J}$ with $\widehat{\phi}$ being its dual, we compute $\langle\ ,\ \rangle_{CT}$ on $\text{Sel}^{\widehat{\phi}}(\widehat{J}) \times \text{Sel}^{\widehat{\phi}}(\widehat{J})$ following the definition of the Cassels-Tate pairing described in Section 2.1.3. Recall we assume all points in $J[2]$ are defined over K. We first show that for all but finitely many places, the local Cassels-Tate pairing is always trivial. Then we give a worked example when $K = \mathbb{Q}$.

2.3.1 Prime bound for Richelot isogeny

In this section, we show that for all but finitely many places, the local Cassels-Tate pairing is always trivial. We first give the following definition.

Definition 2.3.1. Let S be a finite subset of places of K containing all the infinite places. Then for any isogeny $\phi : J \to \widehat{J}$, define:

$$H^1(G_K, J[\phi]; S) := \ker\left(H^1(G_K, J[\phi]) \to \prod_{v \notin S} H^1(G_{K_v^{nr}}, J[\phi])\right).$$

Note that $G_{K_v^{nr}} \subset G_{K_v} \subset G_K$.

Since the defining equations of the Jacobian variety J are derived algebraically from the defining equation of the genus two curve $\mathcal{C}$ with explicit formulae, the set of the places of bad reduction of J is contained in the set of places of bad reduction of $\mathcal{C}$. Unless stated otherwise, we define S to be {places of bad reduction for $\mathcal{C}$} $\cup$ {places dividing $\deg(\phi)$} $\cup$ {infinite places}. We have the following well-known lemma, see [Mil06, Chapter I, Section 6], and [Sch95, Section 3].

Lemma 2.3.2. *For any isogeny ϕ on J, we have*

$$Sel^{\phi}(J) \subset H^1(G_K, J[\phi]; S).$$

Remark 2.3.3.

(i) By Remark 2.2.4 and Definition 2.3.1, under the assumption of this section, we have the following exact sequence:

$$0 \to H^1(G_K, J[\phi]; S) \xrightarrow{f_1} H^1(G_K, J[2]; S) \xrightarrow{f_2} H^1(G_K, \widehat{J}[\widehat{\phi}]; S) \to 0$$

with the formulae the same as the ones given in Propositions 2.2.2 and 2.2.3 under the embeddings. Observe that the element in $H^1(G_K, \widehat{J}[\widehat{\phi}]; S)$ represented by (a, b, c) has a preimage in $H^1(G_K, J[2]; S)$ represented by $(a, 1, b, 1, c)$ via f_2.

(ii) Define $K(S, 2) = \{x \in K^*/(K^*)^2 : \mathrm{ord}_v(x) \text{ is even for all } v \notin S\}$. We get that $\ker\left((K^*/(K^*)^2) \to \prod_{v \notin S} K_v^{nr*}/(K_v^{nr*})^2\right) = K(S, 2)$. This implies, by Lemma 2.3.2, that any element in $\mathrm{Sel}^2(J)$ or $\mathrm{Sel}^{\phi}(J)$ for some Richelot isogeny ϕ has its image in $K(S, 2)^5$ or $K(S, 2)^3$ under the embeddings.

Suppose $a, a' \in \mathrm{Sel}^{\widehat{\phi}}[\widehat{J}]$. Following the definition of the Cassels-Tate pairing and the notation in Section 2.1.3, $\langle a, a' \rangle_{CT}$ is the infinite sum of $\mathrm{inv}_v(\eta_v)$, for all places v of K. We note that $\mathrm{inv}_v(\eta_v)$ is actually trivial for places away from

the set S. This is explained as follows using the commutative diagram below. Here we fix a place v of K.

$$\begin{array}{ccccc}
H^1(G_K, J[\phi]) & \longrightarrow & H^1(G_K, J[2]) & \longrightarrow & H^1(G_K, \widehat{J}[\widehat{\phi}]) \\
\downarrow & & \downarrow{\scriptstyle a_1 \mapsto a_{1_v}} & & \downarrow{\scriptstyle a \mapsto a_v} \\
H^1(G_{K_v}, J[\phi]) & \longrightarrow & H^1(G_{K_v}, J[2]) & \longrightarrow & H^1(G_{K_v}, \widehat{J}[\widehat{\phi}]) \\
\downarrow{\scriptstyle res} & & \downarrow{\scriptstyle res} & \swarrow{\scriptstyle \delta_2} & \uparrow{\scriptstyle \delta_{\widehat{\phi}}} \\
H^1(G_{K_v^{nr}}, J[\phi]) & \longrightarrow & H^1(G_{K_v^{nr}}, J[2]) & & H^0(G_{K_v}, J) = J(K_v).
\end{array}$$

Note that by Proposition 2.2.1 and Lemma 1.4.19, we know computing $\mathrm{inv}(\eta_v)$ requires computing the Hilbert symbol. By Lemma 1.4.18, we know $(x, y)_H = 1$ if the valuations of x, y are both 0 and K has odd residue characteristic.

Under the embedding $\mathrm{Sel}^{\widehat{\phi}}(\widehat{J}) \to (K^*/(K^*)^2)^3$, suppose $a \mapsto (\alpha_1, \alpha_2, \alpha_3)$, $a' \mapsto (\alpha_1', \alpha_2', \alpha_3')$ with $\alpha_i, \alpha_i' \in K(S, 2)$ for all i, by Remark 2.3.3(ii). Let $a_1 \in H^1(G_K, J[2]; S)$ be a lift of a via the map f_2 in Remark 2.3.3(i). Suppose $v \notin S$. We know there exists a representation of the image of $a_{1,v}$ in $(K_v^*/(K_v^*)^2)^5$ such that all its coordinates have valuation 0. Since $J(K_v^{nr}) \xrightarrow{2} J(K_v^{nr})$ is surjective by [AS02, Lemma 3.4], we get the map $H^0(G_{K_v^{nr}}, J) \to H^1(G_{K_v^{nr}}, J[2])$ is the zero map and hence the image of P_v is trivial in $H^1(G_{K_v^{nr}}, J[2])$. This implies $[c_v] = \delta_2(P_v) \in H^1(G_{K_v}, J[2]) \subset (K_v^*/(K_v^*)^2)^5$ has a representation such that all its coordinates have valuation 0. This implies that $[c_v] - a_{1,v} \in H^1(G_{K_v}, J[2]) \subset (K_v^*/(K_v^*)^2)^5$ has a representation such that all its coordinates have valuation 0, denoted by (a, b, c, d, e). Then we lift $([c_v] - a_{1,v}) \in H^1(G_{K_v}, J[2]) \subset (K_v^*/(K_v^*)^2)^5$ to $\rho_v \in H^1(G_{K_v}, \widehat{J}[\widehat{\phi}]) \subset (K_v^*/(K_v^*)^2)^3$ represented by (abd, d, b). Recall that $\eta_v = \rho_v \cup a_v'$ and so $\mathrm{inv}(\eta_v)$ is indeed zero for $v \notin S$ by Proposition 2.2.1 and Lemmas 1.4.18, 1.4.19.

2.3.2 Worked example

We will now explicitly compute the Cassels-Tate pairing for the following Richelot isogeny where the pairing improves the rank bound obtained via descent by Richelot isogeny. We will be using the same notations as in Section 2.1.3 to compute $\langle\ ,\ \rangle_{CT}$ on $\mathrm{Sel}^{\widehat{\phi}}(\widehat{J}) \times \mathrm{Sel}^{\widehat{\phi}}(\widehat{J})$ and our base field K is the field of the rationals, $\mathbb{Q}$.

Let us consider the following genus two curve which is obtained by taking $k = 113$ in [Fly18, Theorem 1]

$$\mathcal{C} : y^2 = (x + 2 \cdot 113)x(x - 6 \cdot 113)(x + 113)(x - 7 \cdot 113),$$

with $G_1 = (x + 2 \cdot 113), G_2 = x(x - 6 \cdot 113), G_3 = (x + 113)(x - 7 \cdot 113)$ and

$$\triangle = \begin{bmatrix} 2 \cdot 113 & 1 & 0 \\ 0 & -6 \cdot 113 & 1 \\ -7 \cdot 113^2 & -6 \cdot 113 & 1 \end{bmatrix} = -7 \cdot 113^2,$$

$$\begin{aligned} L_1 &= G_2' G_3 - G_3' G_2 = -14 \cdot 113^2 (x - 3 \cdot 113), \\ L_2 &= G_3' G_1 - G_1' G_3 = (x + 5 \cdot 113)(x - 113), \\ L_3 &= G_1' G_2 - G_2' G_1 = -(x + 6 \cdot 113)(x - 2 \cdot 113). \end{aligned}$$

So we have a Richelot isogeny ϕ from the J, the Jacobian variety of $\mathcal{C}$, to $\widehat{J}$, the Jacobian variety of the following curve.

$$\widehat{\mathcal{C}} : y^2 = -2(x - 3 \cdot 113)(x + 5 \cdot 113)(x - 113)(x + 6 \cdot 113)(x - 2 \cdot 113)$$

It can be shown that:

$$\begin{aligned} \mathrm{Sel}^{\widehat{\phi}}(\widehat{J}) &=< (2 \cdot 113, -14 \cdot 113, -7), (113, 7, 7 \cdot 113), (113, 113, 1), (2, 2, 1), (1, 7, 7) >, \\ \mathrm{Sel}^{\phi}(J) &=< (113, -7 \cdot 113, -7), (2 \cdot 113, 7, 14 \cdot 113), (113, 1, 113) > . \end{aligned}$$

Now we will compute the Cassels-Tate pairing matrix on $\mathrm{Sel}^{\widehat{\phi}}(\widehat{J}) \times \mathrm{Sel}^{\widehat{\phi}}(\widehat{J})$. Since $(2 \cdot 113, -14 \cdot 113, -7), (113, 7, 7 \cdot 113)$ are images of elements in $J(K)/\widehat{\phi}(\widehat{J}(K))$, they are in the kernel of the Cassels-Tate pairing. So it is sufficient to look at the pairing on $< (113, 113, 1), (2, 2, 1), (1, 7, 7) > \times < (113, 113, 1), (2, 2, 1), (1, 7, 7) >$.

Since the primes of bad reduction are $\{2, 3, 7, 113\}$, we know these are the only primes for which we need to consider by Section 2.3.1. We have the tables below for the local computation that is potentially nontrivial :

Let $a = (113, 113, 1) \in \mathrm{Sel}^{\widehat{\phi}}(\widehat{J})$ then, by the formula given in Proposition 2.2.3, it has a lift $a_1 = (113, 1, 113, 1, 1) \in H^1(G_K, J[2])$. Then for the local calculation, we have the following table:

places v	∞	2	3	7	113
P_v	id	id	$\{(0,0), (-113, 0)\}$	id	$\{(0,0), (-2 \cdot 113, 0)\}$
$\delta_2(P_v)$	id	id	$(-1, 3, -3, -1, -1)$	id	(113, 3 ·113, 3, 1, 1)
$a_{1,v}$	id	id	$(-1, 1, -1, 1, 1)$	id	(113, 1, 113, 1, 1)
$\delta_2(P_v) - a_{1,v}$	id	id	$(1, 3, 3, -1, -1)$	id	(1, 3 ·113, 3 ·113, 1, 1)
ρ_v	id	id	$(-3, -1, 3)$	id	(3·113, 1, 3·113)

Now let $a = (2, 2, 1) \in \mathrm{Sel}^{\widehat{\phi}}(\widehat{J})$ then, by the formula given in Proposition 2.2.3, it has a lift $a_1 = (2, 1, 2, 1, 1) \in H^1(G_K, J[2])$. Then for the local calculation, we have the following table:

places v	∞	2	3	7	113
P_v	id	$\{(0,0),(-2\cdot 113,0)\}$	$\{(0,0),(-113,0)\}$	id	id
$\delta_2(P_v)$	id	$(2,6,3,-1,-1)$	$(-1,3,-3,-1,-1)$	id	id
$a_{1,v}$	id	$(2,\ 1,\ 2,\ 1,\ 1)$	$(-1,1,-1,1,1)$	id	id
$\delta_2(P_v)-a_{1,v}$	id	$(1,6,6,-1,-1)$	$(1,3,3,-1,-1)$	id	id
ρ_v	id	$(-6,-1,6)$	$(-3,-1,3)$	id	id

Lastly let $a=(1,7,7)\in \mathrm{Sel}^{\widehat{\phi}}(\widehat{J})$ then, by the formula given in Proposition 2.2.3, it has a lift $a_1=(1,1,7,1,7)\in H^1(G_K,J[2])$. Then for the local calculation, we have the following table:

places v	∞	2	3	7	113
P_v	id	$\{(-2\cdot 113,0),(-113,0)\}$	id	$\{(-2\cdot 113,0),(-113,0)\}$	id
$\delta_2(P_v)$	id	$(1,2,-2,-2,2)$	id	$(1,\ 1,\ 7,\ 7,\ 1)$	id
$a_{1,v}$	id	$(1,1,-1,1,-1)$	id	$(1,\ 1,\ 7,\ 1,\ 7)$	id
$\delta_2(P_v)-a_{1,v}$	id	$(1,2,2,-2,-2)$	id	$(1,\ 1,\ 1,\ 7,7)$	id
ρ_v	id	$(-1,-2,2)$	id	$(7,\ 7,\ 1)$	id

Following the explicit algorithm for computing the Cassels-Tate pairing, we get that the Cassels-Tate pairing between $(113,113,1)$ and $(2,2,1)$ is the only nontrivial one.

Therefore, we get the 5×5 Cassels-Tate pairing matrix from the 5 generators of $\mathrm{Sel}^{\widehat{\phi}}(\widehat{J})$. More specifically, the ij^{th} entry of the matrix is the Cassels-Tate pairing between the i^{th} and the j^{th} generators of $\mathrm{Sel}^{\widehat{\phi}}(\widehat{J})$, where the generators are in the same order as listed in the Selmer group $\mathrm{Sel}^{\widehat{\phi}}(\widehat{J})$.

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 & 1 \\ 1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Remark 2.3.4. From the computation above, we have shown that the kernel of the Cassels-Tate pairing has dimension 3. We make the following observations:

- We bound the rank of $J(\mathbb{Q})$ via bounding $|J(\mathbb{Q})/\widehat{\phi}(\widehat{J}(\mathbb{Q}))|$ by $|\ker\langle\ ,\ \rangle_{CT}| = 2^3$ instead of $|\mathrm{Sel}^{\widehat{\phi}}(\widehat{J})| = 2^5$. This improves the rank bound of $J(\mathbb{Q})$ from 4 to 2.

- Via Lemma 1.9.2, we have the following exact sequence:

$$0\to J[\phi](\mathbb{Q})\to J[2](\mathbb{Q})\to \widehat{J}[\widehat{\phi}](\mathbb{Q})\to \mathrm{Sel}^{\phi}(J)\to \mathrm{Sel}^2(J)\xrightarrow{\alpha}\mathrm{Sel}^{\widehat{\phi}}(\widehat{J}).$$

It can be shown that $\operatorname{Im}\alpha$ is contained inside $\ker\langle\ ,\ \rangle_{CT}$, the kernel of the Cassels-Tate pairing on $\text{Sel}^{\widehat{\phi}}(\widehat{J}) \times \text{Sel}^{\widehat{\phi}}(\widehat{J})$. Indeed, if $a \in \text{Sel}^{\widehat{\phi}}(\widehat{J})$ is equal to $\alpha(b)$, where $b \in \text{Sel}^2(J)$, then following the earlier notations, we can let $a_1 = b$. Then we can pick $P_v \in J(\mathbb{Q}_v)$ to be the lift of $a_{1,v}$. Therefore, $\delta_2(P_v) - a_{1,v} = 0 \in H^1(G_{\mathbb{Q}_v}, J[2])$ which implies, $a \in \ker\langle\ ,\ \rangle_{CT}$. Hence, we can always bound $|\text{Sel}^2(J)|$ and this bound will be sharp when $\operatorname{Im}\alpha = \ker\langle\ ,\ \rangle_{CT}$, which is the case for the example that we just computed as shown below.

We used MAGMA to compte the size of $\text{Sel}^2(J)$, which is equal to 2^6, and we have the exact sequence:

$$0 \to J[\phi](\mathbb{Q}) \to J[2](\mathbb{Q}) \to \widehat{J}[\widehat{\phi}](\mathbb{Q}) \to \text{Sel}^{\phi}(J) \to \text{Sel}^2(J) \xrightarrow{\alpha} \ker\langle\ ,\ \rangle_{CT} \to 0.$$

$$\text{size} = 2^2 \quad \text{size} = 2^4 \quad \text{size} = 2^2 \quad \text{size} = 2^3 \quad \text{size} = \mathbf{2^6} \quad \text{size} = 2^3$$

So for this example, we have turned the descent by Richelot isogeny into a 2-descent via computing the Cassels-Tate pairing.

Chapter 3

Computing the Equation of the Twisted Kummer

In the remaining chapters of this thesis, our main goal is to give algorithms for explicitly computing the Cassels-Tate pairing on $\text{Sel}^2(J) \times \text{Sel}^2(J)$ for a Jacobian variety J of a genus two curve $\mathcal{C}$. Before getting into the details of these algorithms, this chapter is devoted to giving methods for explicitly computing the twisted Kummer surface that is essential for the algorithms in the later chapters.

This chapter consists of 4 sections. The first section states and proves the notation and algebraic results needed for the later sections. In the next two sections, we describe two methods for explicitly computing the twisted Kummer surface assuming there exists an algorithm that trivializes a matrix algebra specified by its structure constants. Fixing a set of basis $v_1, ..., v_n$ for the underlying vector space of an algebra V of dimension n, the *structure constants* c_{ijk} satisfy $v_i v_j = \sum_{k=1}^{n} c_{ijk} v_k$. Then in the last section, we describe such algorithm in detail. A lot of the results are generalized from the results in the elliptic curve case. We give precise references for the corresponding results in the elliptic curve case in each section. In this chapter, unless stated otherwise, K is a number field and J denotes the Jacobian variety of a genus two curve $\mathcal{C}$ defined by $y^2 = f(x)$ with f a degree 6 polynomial whose coefficients are in K.

3.1 Central Extensions and Theta Groups

In this section, we give definitions and properties of central extensions and theta groups. Most of the results in this section are generalizations of the results in the elliptic curve case in [CFO+08].

3.1.1 Definitions

We give the following definitions. Similar definitions for elliptic curves are in [CFO+08, Section 1].

Definition 3.1.1. A *central extension* of $J[2]$ by $\mathbb{G}_m$ is an exact sequence of group varieties

$$0 \mapsto \mathbb{G}_m \xrightarrow{\alpha} \Lambda \xrightarrow{\beta} J[2] \mapsto 0,$$

with $\mathbb{G}_m$ contained in the center of Λ.

An isomorphism of central extensions $\Lambda_1 \cong \Lambda_2$ is an isomorphism of group varieties $\phi : \Lambda_1 \to \Lambda_2$ such that the following diagram commutes:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \Lambda_1 & \longrightarrow & J[2] & \longrightarrow & 0 \\ & & \downarrow{=} & & \downarrow{\phi} & & \downarrow{=} & & \\ 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \Lambda_2 & \longrightarrow & J[2] & \longrightarrow & 0 \end{array}$$

We usually refer to Λ as a central extension for simplicity. A commutative extension of $J[2]$ by $\mathbb{G}_m$ is a central extension when Λ is an abelian group. The trivial extension, denoted by Λ_0, is induced by $\mathbb{G}_m \times J[2]$. We sometimes call the image of $\mathbb{G}_m$ in Λ the scalars in Λ. For simplicity, we sometimes denote $\alpha(a)$ by a for $a \in \mathbb{G}_m$ and denote $\beta(x)$ by x for $x \in \Lambda$, when the context is clear.

Definition 3.1.2. A theta group $\boldsymbol{\Theta}$ for $J[2]$ is defined with an exact sequence of group varieties

$$0 \mapsto \mathbb{G}_m \xrightarrow{\alpha} \boldsymbol{\Theta} \xrightarrow{\beta} J[2] \mapsto 0,$$

with $\mathbb{G}_m$ contained in the center of $\boldsymbol{\Theta}$ and commutator given by the Weil pairing e_2, i.e. $xyx^{-1}y^{-1} = \alpha(e_2(\beta(x), \beta(y)))$ for all $x, y \in \boldsymbol{\Theta}$.

It is clear that a theta group is a central extension of $J[2]$ by $\mathbb{G}_m$ and an isomorphism of theta groups is an isomorphism of central extensions defined in Definition 3.1.1.

We now describe one special theta group $\boldsymbol{\Theta}_\mathbf{J}$. Consider the morphism $J \xrightarrow{|2\Theta|} \mathcal{K} \subset \mathbb{P}^3$. The translation map τ_P , for $P \in J[2]$, induces an linear isomorphism on $\mathcal{K} \subset \mathbb{P}^3$ as in Remark 1.3.1. This induces a map $\chi_J : J[2] \to \mathrm{PGL}_4$. We define $\boldsymbol{\Theta}_\mathbf{J}$ to be the inverse image of $\chi_J(J[2])$ in GL_4 and we have the following commutating diagram with exact rows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{G}_m & \xrightarrow{\alpha_J} & \boldsymbol{\Theta}_\mathbf{J} & \xrightarrow{\beta_J} & J[2] & \longrightarrow & 0 \\ & & \downarrow{=} & & \downarrow & & \downarrow{\chi_J} & & \\ 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \mathrm{GL}_4 & \longrightarrow & \mathrm{PGL}_4 & \longrightarrow & 0 \end{array}$$

We observe that the first row makes $\boldsymbol{\Theta}_\mathbf{J}$ a central extension. The required commutator making it a theta group follows from a property of the Weil pairing, as discussed in [CF96, Chapter 3 Section 3].

3.1.2 Relationship with $H^1(G_K, J[2])$

In this section, we show that the isomorphism classes of commutative extensions of $J[2]$ by $\mathbb{G}_m$ and the isomorphism classes of theta groups for $J[2]$ are parameterized by $H^1(G_K, J[2])$. The results in the elliptic curve case is in [CFO+08, Section 1] and we generalize the same proofs.

Recall Λ_0 is the trivial central extension $0 \to \mathbb{G}_m \xrightarrow{\alpha_0} \mathbb{G}_m \times J[2] \xrightarrow{\beta_0} J[2] \to 0$ and we have the following lemma.

Lemma 3.1.3.

(i) Let Λ be a commutative extension of $J[2]$ by $\mathbb{G}_m$. Then Λ is a twist of Λ_0.

(ii) Let Λ be a central extension of $J[2]$ by $\mathbb{G}_m$. Then $Aut(\Lambda) \cong J[2]$.

Proof. Statement (i) follows from the fact that every commutative extension of $J[2]$ by $\mathbb{G}_m$ splits over $\bar{K}$ as $\bar{K}^*$ is a divisible group. We observe that any automorphism of Λ maps $x \in \Lambda$ to $\alpha(\pi(\beta(x)))x$ for some homomorphism $\pi : J[2] \to \mathbb{G}_m$. This implies $\mathrm{Aut}(\Lambda) \cong \mathrm{Hom}(J[2], \mathbb{G}_m)$. Hence, we have statement (ii) by the nondegeneracy of the Weil paring e_2.

□

By a corollary of Proposition 1.5.1 [Ser97, Corollary after Chapter III Section 1 Proposition 5], there is a natural bijection between the isomorphism classes of twists of the group variety $\mathbb{G}_m \times J[2]$ and $H^1(G_K, \mathrm{Aut}(\mathbb{G}_m \times J[2]))$.

Now consider Λ_0 as $\mathbb{G}_m \times J[2]$ with the additional structure, the structure of a central extension. We show that there is a natural bijection between the isomorphism classes of twists of Λ_0 and $H^1(G_K, \mathrm{Aut}(\Lambda_0))$. Combining with Lemma 3.1.3, we have the following proposition.

Proposition 3.1.4. *The isomorphism classes of commutative extensions of $J[2]$ by $\mathbb{G}_m$, viewed as twists of Λ_0, are parameterized by $H^1(G_K, J[2])$.*

Moreover, suppose Λ is a twist of Λ_0 with an isomorphism $\phi : \Lambda \to \Lambda_0$ corresponding to $\epsilon \in H^1(G_K, J[2])$. Then $\phi(\phi^{-1})^\sigma$ sends $x \in \Lambda_0$ to $\alpha_0(e_2(\epsilon_\sigma, \beta_0(x)))x$ such that $(\sigma \mapsto \epsilon_\sigma)$ is a cocycle representing ϵ.

Proof. By Lemma 3.1.3, it suffices to show that the isomorphism classes of twists of Λ_0 are parameterized by $H^1(G_K, \mathrm{Aut}(\Lambda_0))$. In particular, suppose Λ is a twist of Λ_0 with an isomorphism $\phi : \Lambda \to \Lambda_0$ corresponding to $\epsilon \in H^1(G_K, \mathrm{Aut}(\Lambda_0))$. Then we show $(\sigma \mapsto \phi(\phi^{-1})^\sigma)$ is a cocycle representing ϵ.

For any twist of Λ_0, $\phi : \Lambda \to \Lambda_0$, we check $\sigma \mapsto \phi(\phi^{-1})^\sigma$ is a cocycle in $Z^1(G_K, \mathrm{Aut}(\Lambda_0))$. We observe that $\mathrm{Aut}(\Lambda_0) \subset \mathrm{Aut}(\mathbb{G}_m \times J[2])$. Let $\epsilon \in H^1(G_K, \mathrm{Aut}(\Lambda_0))$ be represented by the cocycle $(\sigma \mapsto \epsilon_\sigma)$. To construct a twist of Λ_0 by ϵ, we first take the twist Λ of $\mathbb{G}_m \times J[2]$ by ϵ as group varieties. Then the isomorphism $\phi : \Lambda \to \mathbb{G}_m \times J[2]$ with $\phi(\phi^{-1})^\sigma = \epsilon_\sigma$ transfers the structure of central extension on $\mathbb{G}_m \times J[2]$ onto Λ. More explicitly we have

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{G}_m & \xrightarrow{\phi^{-1}\alpha_0} & \Lambda & \xrightarrow{\beta_0\phi} & J[2] & \longrightarrow & 0 \\ & & \downarrow{=} & & \downarrow{\phi} & & \downarrow{=} & & \\ 0 & \longrightarrow & \mathbb{G}_m & \xrightarrow{\alpha_0} & \mathbb{G}_m \times J[2] & \xrightarrow{\beta_0} & J[2] & \longrightarrow & 0 \end{array}$$

Since $\phi(\phi^{-1})^\sigma = \epsilon_\sigma \in \mathrm{Aut}(\Lambda_0)$, we get $\phi^{-1}\alpha_0$ and $\beta_0\phi$ are Galois invariant hence defined over K. The induced group structure on Λ induced by $\mathbb{G}_m \times J[2]$ via ϕ also makes $\mathbb{G}_m$ in the center of Λ and $\phi^{-1}\alpha_0, \beta_0\phi$ group homomorphisms. Therefore, we indeed get a twist of Λ_0 by ϵ.

Hence, we have a well-defined bijection between the isomorphism classes of the twists of Λ_0 and $H^1(G_K, \mathrm{Aut}(\Lambda_0))$ following the routine argument as done in the proofs of Proposition 1.5.10 and Proposition 1.6.1.

□

Similarly we have the following lemma and proposition on theta groups.

Lemma 3.1.5. *Every theta group is a twist of* $\mathbf{\Theta_J}$.

Proof. Let $\mathbf{\Theta}$ be any theta group. Suppose P_1, P_2, P_3, P_4 form a basis of $J[2]$. Since $\bar{K}^*$ is divisible and its images in $\mathbf{\Theta}, \mathbf{\Theta_J}$ are central, we can pick $\lambda_i \in \mathbf{\Theta}$ and $\mu_i \in \mathbf{\Theta_J}$ each of order 2 and a lift of P_i respectively for each i. This induces the isomorphism $\mathbf{\Theta} \to \mathbf{\Theta_J}$ defined over $\bar{K}$ satisfying $\lambda_i \mapsto \mu_i$ for each i.

□

Via Lemmas 3.1.3(ii), Lemma 3.1.5 and the twisting principle, we have the next proposition.

Proposition 3.1.6. *The isomorphism classes of theta groups, as twists of* $\mathbf{\Theta_J}$, *are parameterized by* $H^1(G_K, J[2])$.

Moreover, suppose $\mathbf{\Theta}$ *is a twist of* $\mathbf{\Theta_J}$ *with an isomorphism* $\phi : \mathbf{\Theta} \to \mathbf{\Theta_J}$ *corresponding to* $\epsilon \in H^1(G_K, J[2])$. *Then* $\phi(\phi^{-1})^\sigma$ *sends* $x \in \mathbf{\Theta}$ *to* $\alpha_J(e_2(\epsilon_\sigma, \beta_J(x)))x$ *with* $(\sigma \mapsto \epsilon_\sigma)$ *representing* ϵ.

Proof. The proof is almost identical to the proof of Proposition 3.1.4 and therefore omitted.

□

Construction of $\mathbf{\Theta}_\epsilon$

We now construct a special set of theta groups and show the compatibility of the theta groups and the 2-coverings of J in the case where they correspond to elements in $\mathrm{Sel}^2(J)$. Let $\epsilon \in \mathrm{Sel}^2(J)$. Suppose J_ϵ is a 2-covering of J with an isomorphism $\phi_\epsilon : J_\epsilon \to J$ such that $\phi_\epsilon(\phi_\epsilon^{-1})^\sigma = \tau_{\epsilon_\sigma}$ and $(\sigma \to \epsilon_\sigma)$ is a cocyle representing ϵ. We then have an induced commutative diagram (1.6.2), as discussed in Remark 1.6.3. In particular, ϕ_ϵ induces an linear isomorphism $\psi_\epsilon : \mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$. Then $J[2]$ naturally has an action on $\mathcal{K}_\epsilon \subset \mathbb{P}^3$ induced by its natural action on $\mathcal{K} \subset \mathbb{P}^3$ conjugated by ψ_ϵ. This gives a map $\chi_\epsilon : J[2] \to \mathrm{PGL}_4$. Hence, similar to $\mathbf{\Theta_J}$, we define a theta group $\mathbf{\Theta}_\epsilon$ to be the inverse image of $\chi_\epsilon(J[2])$ in GL_4 via the following similar commutative diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{G}_m & \xrightarrow{\alpha_\epsilon} & \mathbf{\Theta}_\epsilon & \xrightarrow{\beta_\epsilon} & J[2] & \longrightarrow & 0 \\ & & \downarrow{=} & & \downarrow & & \downarrow{\chi_\epsilon} & & \\ 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \mathrm{GL}_4 & \longrightarrow & \mathrm{PGL}_4 & \longrightarrow & 0 \end{array}$$

Lemma 3.1.7. *The theta group $\mathbf{\Theta}_\epsilon$ constructed above is the twist of $\mathbf{\Theta_J}$ by ϵ.*

Proof. We lift ψ_ϵ to a matrix $B \in \mathrm{GL}_4$. It can be checked that $M \mapsto BMB^{-1}$ defines an isomorphism $\Psi : \mathbf{\Theta}_\epsilon \to \mathbf{\Theta_J}$. Since B is induced by ϕ_ϵ with $\phi_\epsilon(\phi_\epsilon^{-1})^\sigma = \tau_{\epsilon_\sigma}$, we get $\beta_\epsilon(B(B^{-1})^\sigma) = \epsilon_\sigma$. Therefore, $\Psi(\Psi^{-1})^\sigma$ is an automorphism of $\mathbf{\Theta_J}$ such that $N \mapsto B(B^{-1})^\sigma N B^\sigma B^{-1} = e_2(\epsilon_\sigma, \beta_\epsilon(N))N$. This implies that $\mathbf{\Theta}_\epsilon$ indeed corresponds to ϵ by Proposition 3.1.6.

□

Remark 3.1.8. By Proposition 3.1.6 and Lemma 3.1.7, we know different choices of the isomorphism $\phi_\epsilon : J_\epsilon \to J$ such that $(J_\epsilon, [2] \circ \phi_\epsilon)$ is the 2-covering for J corresponding to ϵ and different choices of the induced ψ_ϵ give rise to isomorphic theta groups.

3.1.3 Étale algebra

Definition 3.1.9. Let K be a field, a K-algebra L is *étale* if it is isomorphic to a finite product of finite separable field extensions of K.

In later discussions in this thesis, we will be studying the following K-algebra:

Let R denote the set $\mathrm{Map}_K(J[2], \bar{K}) := \{\phi : J[2] \to \bar{K}$ such that $(\phi(P))^\sigma = \phi(P^\sigma)$, for all $P \in J[2], \sigma \in G_K\}$, namely the set of all Galois equivariant maps from $J[2]$ to $\bar{K}$. We also define the algebra $\bar{R} = R \otimes_K \bar{K} = \mathrm{Map}(J[2], \bar{K})$ and let $R^*, \bar{R}^*$ denote the unit groups of $R, \bar{R}$ respectively, which are $\mathrm{Map}_K(J[2], \bar{K}^*)$ and $\mathrm{Map}(J[2], \bar{K}^*)$.

Proposition 3.1.10. *Suppose A is a finite set with a action by G_K. Let L denote $Map_K(A, \bar{K})$, the set of Galois equivariant maps from A to $\bar{K}$. Then L is an étale algebra with* $\dim L = |A|$.

Proof. Suppose G_K acts transitively on a subset $A_1 \subset A$. Pick $a \in A_1$. Any $r \in \mathrm{Map}_K(A_1, \bar{K})$ is determined by the image of a. Let $S \subset G_K$ be the stabilizer of a. We know $r(a) \in \bar{K}^S$ if $r \in \mathrm{Map}_K(A_1, \bar{K})$. Hence $\mathrm{Map}_K(A_1, \bar{K}) \cong \bar{K}^S$, where $\bar{K}^S$ is a finite extension of K with degree of extension $\mathrm{index}_S G_K$. This implies, by the Orbit-Stabilizer Theorem,

$$\dim \mathrm{Map}_K(A_1, \bar{K}) = [\bar{K}^S : K] = \mathrm{index}_S G_K = |A_1|.$$

Hence, by writing A as a disjoint union of Galois orbits, we have that L is isomorphic to a product of finite field extensions of K, one for each G_K-orbit in A and $\dim L = |A|$.

□

Applying Proposition 3.1.10 to the set $J[2]$ gives the corollary below.

Corollary 3.1.11. *R is an étale algebra and* $\dim R = 16$.

3.1.4 Invariants of central extensions

In this section, we define two invariants of a central extension. First, we give definitions and notation for the following group homomorphisms. These group homomorphisms in the case of elliptic curves are defined in [CFO+08, Section 3].

The Weil pairing $e_2 : J[2] \times J[2] \to \mu_2$ determines an injection $w : J[2] \to \mu_2(\bar{R}) \subset \bar{R}^*$ with $T \mapsto e_2(T, -)$. From the definition and the non-degeneracy of the Weil pairing, we know that $w(T)$ for $T \in J[2]$ is actually a homomorphism and all homomorphisms arise this way. We note that $R \otimes R$ is the algebra of Galois equivariant maps from $J[2] \times J[2]$ into $\bar{K}$ and $\bar{R} \otimes_{\bar{K}} \bar{R} = (R \otimes R) \otimes_K \bar{K}$ is the algebra of all such maps. Define $\partial : \bar{R}^* \to (\bar{R} \otimes_{\bar{K}} \bar{R})^*$ such that

$$\partial\alpha(T_1, T_2) = \frac{\alpha(T_1)\alpha(T_2)}{\alpha(T_1 + T_2)},$$

and we have an exact sequence:

$$0 \to J[2] \xrightarrow{w} \bar{R}^* \xrightarrow{\partial} (\bar{R} \otimes_{\bar{K}} \bar{R})^*. \tag{3.1.1}$$

By a generalized version of Hilbert's theorem 90 [Ser79, Chapter X, Section 1 Exercise 2], which says $H^1(G_K, M^*) = 0$ for M a finite-dimensional unitary K-algebra, we have $H^1(G_K, \bar{R}^*) = 0$. Suppose $\epsilon \in H^1(G_K, J[2])$ is represented by $(\sigma \mapsto \epsilon_\sigma)$. Let w_* denote the natural map $H^1(G_K, J[2]) \to H^1(G_K, \bar{R}^*)$ induced by w. Since $H^1(G_K, \bar{R}^*) = 0$, we know $w_*(\epsilon)$ is a co-boundary, i.e. $w(\epsilon_\sigma) = \sigma(\gamma)/\gamma$ for some $\gamma \in \bar{R}^*$. Then let $\alpha = \gamma^2$ and $\rho = \partial\gamma$. Since they are both Galois invariant, they are in R^* and $(R \otimes R)^*$ respectively. Therefore we can define the following maps.

$$\begin{aligned} w_1 : H^1(G_K, J[2]) &\to R^*/(R^*)^2, \\ \epsilon &\mapsto \alpha(R^*)^2 \end{aligned}$$

$$\begin{aligned} w_2 : H^1(G_K, J[2]) &\to (R \otimes R)^*/\partial R^*. \\ \epsilon &\mapsto \rho \partial R^* \end{aligned}$$

Lemma 3.1.12. *w_1, w_2 defined above are well defined group homomorphisms.*

Proof. These two maps are well defined. If we change $(\sigma \mapsto \epsilon_\sigma)$ by a co-boundary, say $(\sigma \mapsto \sigma(T) - T)$, then γ is multiplied by $w(T)$. Since $w(T)^2 = 1$ and $\partial(w(T)) = 1$, the values of α and ρ are unchanged. The only remaining freedom is to multiple γ by an element in R^*, and it results in multiplying α and ρ by elements in $(R^*)^2$ and ∂R^*. It can be checked that they are indeed group homomorphisms.

□

Remark 3.1.13. We observe that w_2 is induced from the long exact sequence associated to (3.1.1) and w_1 is in fact the composition of the following:

$$w_1 : H^1(G_K, J[2]) \xrightarrow{w_*} H^1(G_K, \mu_2(\bar{R}^*)) \to R^*/(R^*)^2,$$

where the second map is the Kummer isomorphism induced by the fact that $H^1(G_K, \bar{R}^*) = 0$.

The first and second invariants

Now consider a central extension Λ with the following exact sequence:

$$0 \to \mathbb{G}_m \to \Lambda \to J[2] \to 0.$$

By Hilbert's Theorem 90, we know there always exists a Galois equivariant section $\phi : J[2] \to \Lambda$. In general ϕ is not a group homomorphism and the different choices of ϕ differ by elements in R^*. We define the first and second invariants of Λ as follows.

The first invariant is $\text{inv}_1(\Lambda) = \alpha(R^*)^2$, where $\alpha \in R^*$ satisfies

$$\phi(T)^2 = \alpha(T),$$

for all $T \in J[2]$.

The second invariant is $\text{inv}_2(\Lambda) = \rho\partial R^*$, where $\rho \in (R \otimes R)^*$ satisfies

$$\phi(T_1)\phi(T_2) = \rho(T_1, T_2)\phi(T_1 + T_2),$$

for all $T_1, T_2 \in J[2]$.

Remark 3.1.14. Notice that since the different choices of ϕ differ by elements in R^*, $\text{inv}_1(\Lambda)$ and $\text{inv}_2(\Lambda)$ depend only on Λ and not on the choice of section ϕ.

Recall that Proposition 3.1.4 shows that the isomorphism classes of commutative extensions of $J[2]$ by $\mathbb{G}_m$, as twists of Λ_0, are parameterized by $H^1(G_K, J[2])$. The lemma below shows the relationship between the group homomorphisms w_1, w_2 and the invariants of a commutative extension. The proof is the same as the elliptic cure case, see [CFO+08, Lemma 3.3].

Lemma 3.1.15. *Let Λ be the twist of Λ_0 that corresponds to $\epsilon \in H^1(G_K, J[2])$. Then*

$$inv_1(\Lambda) = w_1(\epsilon) \text{ and } inv_2(\Lambda) = w_2(\epsilon).$$

Proof. Let $\psi : \Lambda \to \Lambda_0$ denote the twist and $\phi_0 : J[2] \to \Lambda_0$ be the natural section for Λ_0. By Proposition 3.1.4, we know that $\psi(\psi^{-1})^\sigma : x \mapsto \alpha_0(e_2(\epsilon_\sigma, \beta_0(x)))x$ with $(\sigma \mapsto \epsilon_\sigma)$ representing ϵ. Since $w(\epsilon_\sigma) = \sigma(\gamma)/\gamma$ for some $\gamma \in \bar{R}^*$, it can be shown that

$$\phi : J[2] \to \Lambda; T \mapsto \gamma(T)\psi^{-1}(\phi_0(T))$$

is a Galois equivariant section for Λ. Hence, the results of the lemma follow from definition of the invariants.

□

We also have the lemma below on the relationship between the invariants of $\mathbf{\Theta_J}$ and those of any theta group $\mathbf{\Theta}$. The proof is very similar to the proof of

Lemma 3.1.15 and therefore omitted. The result in the elliptic curve case is in [CFO+08, Lemma 3.10].

Lemma 3.1.16. *Let $\mathbf{\Theta}$ be the twist of $\mathbf{\Theta_J}$ by $\epsilon \in H^1(G_K, J[2])$. Then*

$$inv_1(\mathbf{\Theta}) = w_1(\epsilon) inv_1(\mathbf{\Theta_J}) \text{ and } inv_2(\mathbf{\Theta}) = w_2(\epsilon) inv_2(\mathbf{\Theta_J}).$$

3.2 The Naive Method

In this section, unless stated otherwise, we fix $\epsilon \in \mathrm{Sel}^2(J)$ and $(J_\epsilon, \pi_\epsilon)$ the 2-covering of J corresponding to ϵ. We will describe a method for explicitly computing a linear change of coordinates on $\mathbb{P}^3$, denoted by ψ_ϵ, in the commutative diagram of the base Brauer-Severi diagram $[J \to \mathbb{P}^3]$ and its twist $[J_\epsilon \to \mathbb{P}^3]$ that corresponds to ϵ. Let $\mathcal{K}_\epsilon$ denote the twisted Kummer surface which is $\psi_\epsilon^{-1}(\mathcal{K}) \subset \mathbb{P}^3$. So $\psi_\epsilon : \mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ and there exists an isomorphism $\phi_\epsilon : J_\epsilon \to J$ such that $[2] \circ \phi_\epsilon = \pi_\epsilon$, with a commutative diagram (1.6.2) in Lemma 1.6.3 corresponding to ϵ. Note that this is equivalent to finding a linear isomorphism $\psi_\epsilon : \mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ such that $(\sigma \mapsto \psi_\epsilon(\psi_\epsilon^{-1})^\sigma)$ gives a cocycle for ϵ. Indeed, for an isomorphism $\phi_\epsilon : J_\epsilon \to J$ such that $(\sigma \mapsto \phi_\epsilon(\phi_\epsilon^{-1})^\sigma)$ gives the same cocycle as the one given by ψ_ϵ, we have $J_\epsilon \xrightarrow{\psi_\epsilon^{-1} k \phi_\epsilon} \mathcal{K}_\epsilon \subset \mathbb{P}^3$ defined over K as required since $(\psi_\epsilon^{-1} k \phi_\epsilon)^\sigma = \psi_\epsilon^{-1} \circ \psi_\epsilon(\psi_\epsilon^{-1})^\sigma \circ k \circ \phi_\epsilon^\sigma \phi_\epsilon^{-1} \circ \phi_\epsilon = \psi_\epsilon^{-1} k \phi_\epsilon$ with $k : J \xrightarrow{|2\Theta|} \mathcal{K}$. For simplicity, we sometimes call such ψ_ϵ as a linear isomorphism $\mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ corresponding to ϵ.

3.2.1 Action of $J[2]$

In Remark 1.3.1, we showed that τ_P gives a linear isomorphism on $\mathcal{K} \subset \mathbb{P}^3$ for any $P \in J[2]$. Recall the theta group $0 \to \mathbb{G}_m \to \mathbf{\Theta_J} \to J[2] \to 0$ defined in Section 3.1.1 is precisely the subset of GL_4 consisting of elements representing the action of some $P \in J[2]$ on $\mathcal{K} \subset \mathbb{P}^3$. In particular, we have the following lemma.

Lemma 3.2.1.

(i) Let $P \mapsto M_P$ be a section for $\mathbf{\Theta_J} \to J[2]$. Then $\{M_P, P \in J[2]\}$ forms a basis of $Mat_4(\bar{K})$ and the set of matrices in $PGL_4(\bar{K})$ that commute with M_P in $PGL_4(\bar{K})$ for all $P \in J[2]$ is $\{[M_P], P \in J[2]\}$.

(ii) There exists an explicit Galois equivariant section for $\mathbf{\Theta_J} \to J[2]$. The formula for a Galois equivariant section for $\mathbf{\Theta_J} \to J[2]$ can be found in [CF96, Chapter 3 Section 2] *with $M_{\mathcal{O}_J} = I$.*

Proof. Let $P \mapsto M_P$ be a section for $\mathbf{\Theta_J} \to J[2]$. The non-degeneracy of the Weil pairing gives the linear independence of M_P. Then they form a basis of $\mathrm{Mat}_4(\bar{K})$ by a dimension count. Suppose there exists $\lambda_P \in \bar{K}^*$ such that $\sum_{P\in J[2]} \lambda_P M_P$ commutes with M_Q in $\mathrm{PGL}_4(\bar{K})$ for all $Q \in J[2]$. Then there exists $c_Q \in \bar{K}$ such that $\sum_{P\in J[2]} \lambda_P(e_2(P,Q)-c_Q)M_Q M_P = 0$ for any $Q \in J[2]$. Since $M_Q M_P$ represents the action of $P+Q$ on $\mathcal{K}$, it is a multiple of M_{P+Q}. Hence, $\{M_P M_Q, P \in J[2]\}$ also forms a basis for $\mathrm{Mat}_4(\bar{K})$ for any $Q \in J[2]$, which means for $\lambda_P(e_2(P,Q)-c_Q) = 0$ for all $P, Q \in J[2]$. Suppose there exists more than one $P \in J[2]$ such that $\lambda_P \neq 0$, we derive a contradiction to the non-degeneracy of the Weil pairing. This completes the proof for (i).

□

From now on, we always let $M_P \in \mathrm{GL}_4(\bar{K})$ for $P \in J[2]$ equal to the one given in Lemma 3.2.1(ii) with explicit formulae in [CF96, Chapter 3 Section 2], which gives a Galois equivariant section for $\mathbf{\Theta_J} \to J[2]$.

Suppose we fix $\mathcal{K}_\epsilon$ as a subvariety in $\mathbb{P}^3$ and are given a linear isomorphism $\psi_\epsilon : \mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ corresponding to ϵ. We now consider the automorphisms on $\mathcal{K}_\epsilon \subset \mathbb{P}^3$ induced by the action of points in $J[2]$, which are also the conjugations of $[M_P]$ by ψ_ϵ. Recall the theta group $\mathbf{\Theta}_\epsilon$ for $J[2]$, defined in Section 3.1.2, is precisely the subgroup of $\mathrm{GL}_4(\bar{K})$ consisting of elements representing the action of translation by some $P \in J[2]$ on $\mathcal{K}_\epsilon \subset \mathbb{P}^3$ and is a twist of $\mathbf{\Theta_J}$ by ϵ as shown in Lemma 3.1.7. Let $P \mapsto M'_P$ be a section for $\mathbf{\Theta}_\epsilon \to J[2]$. we know M'_P represents the action of P on $\mathcal{K}_\epsilon$ and it is equal to M_P conjugated by ψ_ϵ in $\mathrm{PGL}_4(\bar{K})$. Since $\{M_P, P \in J[2]\}$ forms a basis for $\mathrm{Mat}_4(\bar{K})$ by Lemma 3.2.1(i), $\{M'_P, P \in J[2]\}$ also forms a basis for $\mathrm{Mat}_4(\bar{K})$.

Lemma 3.2.2. *Fix $\mathcal{K}_\epsilon$ as a subvariety in $\mathbb{P}^3$. Let $\psi_\epsilon, \psi'_\epsilon : \mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ be two different isomorphisms as above. Then $\psi'_\epsilon \psi_\epsilon^{-1}$ is the action of translation by some $P \in J[2]$ on $\mathcal{K} \subset \mathbb{P}^3$. This implies there exist precisely 16 isomorphisms $\mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ corresponding to ϵ and the construction of $\mathbf{\Theta}_\epsilon$ is independent of the choice of ψ_ϵ corresponding to ϵ. Let $P \mapsto M'_P$ be a section for $\mathbf{\Theta}_\epsilon \to J[2]$. Suppose $\psi : \mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ is a linear isomorphism represented by $A \in Mat_4(\bar{K})$. We have (i) if and only if (ii), where*

(i) ψ corresponds to ϵ,

(ii) $M'_P = A^{-1} M_P A \in PGL_4(\bar{K})$ for all $P \in J[2]$.

Moreover, suppose $\mathcal{K}_\epsilon$ can be embedded as subvarieties $\mathcal{K}_1$ and $\mathcal{K}_2$ in $\mathbb{P}^3$ which both give rise to the same theta group $\mathbf{\Theta}_\epsilon \subset GL_4(\bar{K})$. Then $\mathcal{K}_1 = \mathcal{K}_2 \subset \mathbb{P}^3$. Hence, the different ways of viewing $\mathcal{K}_\epsilon$ as a subvariety in $\mathbb{P}^3$ one to one correspond to the different theta groups $\mathbf{\Theta}_\epsilon \subset GL_4(\bar{K})$ constructed.

Proof. Suppose $\psi_\epsilon, \phi_\epsilon$ and $\psi'_\epsilon, \phi'_\epsilon$ both satisfy the commutative diagram (1.6.2) corresponding to ϵ. Then, $\phi'_\epsilon \phi_\epsilon^{-1}$ is an automorphism of the base Brauer-Severi

diagram, which implies $\phi'_\epsilon\phi_\epsilon^{-1}$ is a translation by a two-torsion point on J by Lemma 1.5.2. Hence, $\psi'_\epsilon\psi_\epsilon^{-1}$ is the action of translation by some $P \in J[2]$ on $\mathcal{K} \subset \mathbb{P}^3$ and the automorphism on $\mathcal{K}_\epsilon$ induced by $P \in J[2]$ is independent of the choice of ψ_ϵ corresponding to ϵ.

It is straightforward that (i) implies (ii). Now suppose ψ satisfies (ii). Let $\psi_\epsilon : \mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$, represented by $A_\epsilon \in \mathrm{Mat}_4(\bar{K})$, be an isomorphism corresponding to ϵ and hence it satisfies (ii). Then AA_ϵ^{-1} commute with M_Q in $\mathrm{PGL}_4(\bar{K})$, for all $Q \in J[2]$. By Lemma 3.2.1(i), we know $A_\epsilon = M_P A$ in $\mathrm{PGL}_4(\bar{K})$ for some $P \in J[2]$. Suppose $\phi_\epsilon : J_\epsilon \to J$ and ψ_ϵ satisfy the commutative diagram (1.6.2). Then $\phi = \tau_{-P} \circ \phi_\epsilon$ and ψ satisfy the commutative diagram (1.6.2) which gives (i).

Moreover, let $\psi_1 : \mathcal{K}_1 \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3, \psi_2 : \mathcal{K}_2 \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ be isomorphisms corresponding to ϵ represented by $A_1, A_2 \in \mathrm{GL}_4(\bar{K})$ respectively. Since they give rise to the same theta group $\mathbf{\Theta}_\epsilon \subset \mathrm{GL}_4$, we have $A_1^{-1}M_Q A_1 = A_2^{-1}M_Q A_2 \in \mathrm{PGL}_4(\bar{K})$ and so $A_1A_2^{-1}$ commute with M_Q in $\mathrm{PGL}_4(\bar{K})$, for all $Q \in J[2]$. This, by Lemma 3.2.1(i), implies $\psi_1\psi_2^{-1}$ is the action of translation by some $P \in J[2]$ on $\mathcal{K} \subset \mathbb{P}^3$. Hence, $\mathcal{K}_1 = \mathcal{K}_2 \subset \mathbb{P}^3$.

□

3.2.2 Computing the invariants of $\mathbf{\Theta}_\epsilon$

In this section, we compute $\mathrm{inv}_1(\mathbf{\Theta}_\epsilon), \mathrm{inv}_2(\mathbf{\Theta}_\epsilon)$ for $\epsilon \in \mathrm{Sel}^2(J)$ and explain how they are related to finding an explicit twist of $\mathcal{K}$ corresponding to ϵ. By Lemma 3.1.16, we need to study $w_1(\epsilon)$ and $w_2(\epsilon)$. Recall our genus two curve $\mathcal{C}$ is defined by $y^2 = f(x)$ with $\deg f = 6$. Let $L = K[x]/(f)$ and let $\Omega = \{\omega_1, ..., \omega_6\}$ denote the 6 roots of f. As discussed in Section 1.10.1, we know there is a homomorphism $\mathrm{Sel}^2(J) \to L^*/(L^*)^2K^*$. We have the following lemma that gives explicit formulae for w_1 and w_2.

Lemma 3.2.3. *Let $\delta \in L^*$ represent the image of $\epsilon \in Sel^2(J)$ in $L^*/(L^*)^2K^*$ with $N(\delta) = n^2$. Suppose ϵ is represented by (δ, m) under the identification in Remark 1.10.6, with $m = n$ or $m = -n$. Let $d_i \in \bar{K}$ such that $d_i^2 = \delta(\omega_i)$ and $\prod_{i=1}^6 d_i = m$. Define $\gamma \in \bar{K}^*$ such that $\gamma(\mathcal{O}_J) = 1$ and $\gamma(\{(\omega_i, 0), (\omega_j, 0)\}) = d_i d_j$ for $i \neq j$. We have $w(\epsilon_\sigma) = \sigma(\gamma)/\gamma$ for all $\sigma \in G_K$ and $(\sigma \mapsto \epsilon_\sigma)$ is a cocycle representing ϵ.*

Proof. As discussed in Section 1.10.1, we have isomorphism $\bar{L} \cong \mathrm{Map}(\Omega, \bar{K}) \cong \bar{K}^6$ where the first natural isomorphism is Galois equivariant and the second isomorphism is evaluation at the 6 roots in a fixed order $\omega_1, ..., \omega_6$. Via the first isomorphism, we get $L \cong \mathrm{Map}_K(\Omega, \bar{K})$. Let $\delta_i \in \bar{L}$ that sends ω_i to -1 and sends ω_j to 1 for $i \neq j$. Recall we also defined $M \subset \mu_2(\bar{L}) = \ker(\mu_2(\bar{L}) \xrightarrow{N} \mu_2(\bar{K}))$ where $\delta_i\delta_j$ form a basis for M as a $\mathbb{F}_2$-vector space, $\beta : M \to J[2]$ that sends $\delta_i\delta_j$ to $\{(\omega_i, 0), (\omega_j, 0)\}$, and $\alpha : J[2] \to \mu_2(\bar{L})/\mu_2(\bar{K})$ that sends $\{(\omega_i, 0), (\omega_j, 0)\}$ to

$\delta_i\delta_j$.

We have the following commutative diagram where the top half appears in (1.10.1):

$$\begin{array}{ccc} M & \longrightarrow & \mu_2(\bar{L}) \\ \downarrow{\scriptstyle \beta} & & \downarrow \\ J[2] & \xrightarrow{\alpha} & \frac{\mu_2(\bar{L})}{\mu_2(\bar{K})} \\ \downarrow{\scriptstyle =} & & \downarrow \\ J[2] & \xrightarrow{w} & \mu_2(\bar{R}) \end{array} \tag{3.2.1}$$

where $\mu_2(\bar{L})/\mu_2(\bar{K}) \to \mu_2(\bar{R})$ sends f to the map $\{(\omega_i,0),(\omega_j,0)\} \mapsto f(\omega_i)f(\omega_j)$. The commutative diagram (3.2.1) above gives the commutative diagram on the cochains. Let $d_i \in \bar{K}$ such that $d_i^2 = \delta(\omega_i)$ and $\prod_{i=1}^6 d_i = m$. There exists $\zeta \in \bar{L}$ satisfying $\zeta(\omega_i) = d_i$. This implies that $\zeta^2 = \delta$ and $N(\zeta) = m$. By Proposition 1.10.4, we have the image of $(\sigma \mapsto \sigma(\zeta)/\zeta) \in C^1(G_K, M)$ induced by β, is a cocycle $(\sigma \mapsto \epsilon_\sigma) \in C^1(G_K, J[2])$ representing ϵ. Then via a diagram chase, we get $w(\epsilon_\sigma) = \sigma(\gamma)/\gamma$ where $\gamma(\{(\omega_i,0),(\omega_j,0)\}) = d_id_j$ for $i \neq j$ and $\gamma(\mathcal{O}_J) = 1$ as required.

□

Remark 3.2.4. Follow the notation in Lemma 3.2.3. By Lemma 3.2.3 and the definitions of w_1, w_2, we know $w_1(\epsilon) = \alpha(R^*)^2$ with $\alpha = \gamma^2 \in R$ and $w_2(\epsilon) = \rho\partial R^*$ with $\rho = \partial\gamma \in (R \otimes R)^*$. In particular, $\alpha \in R$ is defined by

$$\begin{aligned} \mathcal{O}_J &\mapsto 1 \\ \{(\omega_i,0),(\omega_j,0)\} &\mapsto \delta(\omega_i)\delta(\omega_j); \end{aligned}$$

and $\rho \in (R \otimes R)^*$ is defined by

$$\begin{aligned} (\mathcal{O}_J, \mathcal{O}_J) &\mapsto 1, \\ (\{(\omega_i,0),(\omega_j,0)\}, \mathcal{O}_J) &\mapsto 1, \\ (\{(\omega_i,0),(\omega_j,0)\}, \{(\omega_i,0),(\omega_j,0)\}) &\mapsto \delta(\omega_i)\delta(\omega_j), \\ (\{(\omega_i,0),(\omega_j,0)\}, \{(\omega_i,0),(\omega_k,0)\}) &\mapsto \delta(\omega_i), \end{aligned}$$

for distinct i, j, k and

$$(\{(\omega_i,0),(\omega_j,0)\}, \{(\omega_k,0),(\omega_l,0)\}) \mapsto \frac{m}{\delta(\omega_p)\delta(\omega_q)},$$

where (i,j,k,l,p,q) is a permutation of $(1,2,3,4,5,6)$. Note that $\partial\gamma(P,P) = \gamma^2(P)$ for any $P \in J[2]$.

Remark 3.2.5. Note that in the statement of Lemma 3.2.3, d_i are defined up to a choice of sign. From the explicit formulae in Remark 3.2.4, γ^2 and $\partial\gamma$ are independent of the choices of sign.

We now show that to compute a linear isomorphism $\psi_\epsilon : \mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ corresponding to ϵ, it suffices to first compute a set of basis $\{N'_P, P \in J[2]\}$ for $\mathrm{Mat}_4(\bar{K})$ such that

$$N'_{P_1} N'_{P_2} = \xi_\epsilon(P_1, P_2) N'_{P_1+P_2} \text{ and } \sigma(N_P)' = N'_{\sigma(P)},$$

where $\xi_\epsilon = \rho\xi \in (R \otimes R)^*$ with $M_{P_1} M_{P_2} = \xi(P_1, P_2) M_{P_1+P_2}$ and ρ explicitly given in Remark 3.2.4. Then one such ψ_ϵ is represented by $B \in \mathrm{Mat}_4(\bar{K})$ with $N'_P = B^{-1} M_P B \in \mathrm{PGL}_4(\bar{K})$ for all $P \in J[2]$.

Consider $\mathcal{K}_\epsilon$ as a fixed subvariety of $\mathbb{P}^3$ and the theta group $\mathbf{\Theta}_\epsilon \subset \mathrm{GL}_4(\bar{K})$ representing the action of $J[2]$ on $\mathcal{K}_\epsilon \subset \mathbb{P}^3$ as defined in Section 3.1.2. By Lemma 3.1.16 and Remark 3.2.4, we know there exists a Galois equivariant section for $\mathbf{\Theta}_\epsilon \to J[2]$, given by $P \mapsto M'_P$, such that $M'_{P_1} M'_{P_2} = \xi_\epsilon(P_1, P_2) M'_{P_1+P_2}$. We also know that there exists $A \in \mathrm{Mat}_4(\bar{K})$ representing an linear isomorphism $\mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ corresponding to ϵ such that $M'_P = A^{-1} M_P A \in \mathrm{PGL}_4(\bar{K})$ for all $P \in J[2]$.

Suppose we have a set of basis $\{N'_P, P \in J[2]\}$ for $\mathrm{Mat}_4(\bar{K})$ such that $N'_{P_1} N'_{P_2} = \xi_\epsilon(P_1, P_2) N'_{P_1+P_2}$ and $\sigma(N_P)' = N'_{\sigma(P)}$ for all $P \in J[2]$. Then the automorphism of $\mathrm{Mat}_4(\bar{K})$ given by $M'_P \mapsto N'_P$ restricts to an automorphism of $\mathrm{Mat}_4(K)$ which is the conjugation by some $C \in \mathrm{Mat}_4(K)$ by the Noether Skolem theorem. This implies that $N'_P = C^{-1} M'_P C$ and $AC \in \mathrm{Mat}_4(\bar{K})$ also represents an linear isomorphism $\mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ corresponding to ϵ with a change of coordinates for the ambient space of $\mathcal{K}_\epsilon$. Moreover, by Lemma 3.2.2, different choices of C give the same $\mathcal{K}_\epsilon \subset \mathbb{P}^3$ and finding ψ_ϵ is equivalent to solving for a matrix $B \in \mathrm{Mat}_4(\bar{K})$ with $N'_P = B^{-1} M_P B \in \mathrm{PGL}_4(\bar{K})$ for all $P \in J[2]$.

Remark 3.2.6. By the discussion above, we know that any set of basis $\{N'_P, P \in J[2]\}$ for $\mathrm{Mat}_4(\bar{K})$ such that $N'_{P_1} N'_{P_2} = \xi_\epsilon(P_1, P_2) N'_{P_1+P_2}$ and $\sigma(N_P)' = N'_{\sigma(P)}$ for all $P \in J[2]$ can be taken to represent the action of $J[2]$ on the image of some embedding of $\mathcal{K}_\epsilon$ in $\mathbb{P}^3$. Therefore, we also denote N'_P by M'_P for simplicity.

3.2.3 Algorithm for the naive method

In this section, we describe a method for computing a linear isomorphism $\mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ corresponding to ϵ, when the base field is $\mathbb{Q}$. As discussed at the end of Section 3.2.2, we do this by explicitly computing a set of basis $\{M'_P, P \in J[2]\}$ for $\mathrm{Mat}_4(\bar{K})$ such that $M'_{P_1} M'_{P_2} = \xi_\epsilon(P_1, P_2) M'_{P_1+P_2}$ and $\sigma(M_P)' = M'_{\sigma(P)}$ for all $P \in J[2]$. Then one such ψ_ϵ is represented by

$B \in \mathrm{Mat}_4(\bar{K})$ with $M'_P = B^{-1}M_P B \in \mathrm{PGL}_4(\bar{K})$ for all $P \in J[2]$. We call this the naive method and we will describe it assuming that there is an algorithm that trivializes a matrix algebra specified by its structure constants. More precisely, the algorithm solves Problem 3.4.1 in the case $n = 4$. First, we consider a change of basis of $\{M'_P, P \in J[2]\}$ for $\mathrm{Mat}_4(\bar{K})$ in the following lemma.

Lemma 3.2.7. *Let $r_1, ..., r_{16}$ be a basis for R. Fix an ordering $P_1, ..., P_{16}$ of $J[2]$. Define $\mathbf{P} \in GL_{16}(\bar{K})$, where $\mathbf{P}_{ij} = r_i(P_j)$. Change the basis $\{M'_P, P \in J[2]\}$ for $Mat_4(\bar{K})$ via $\mathbf{P}$ gives $M_i := \sum_{P\in J[2]} r_i(P)M'_P$ for all $i \in \{1, 2, ..., 16\}$. Moreover, $M_1, ..., M_{16}$ also form a K-basis for $Mat_4(K)$ and the structure constants with respect to $M_1, ..., M_{16}$ are defined over K.*

Proof. For $r \in \bar{R}$, it can be checked that $\sum_{P\in J[2]} r(P)M'_P \in \mathrm{Mat}_4(K)$ if and only if $r \in R$. This implies, $M_i \in \mathrm{Mat}_4(K)$ for all $i = 1, ...16$. Since $r_1, ..., r_{16}$ form a basis for R, it can be checked that the matrix $\mathbf{P}$ is indeed invertible. Then the rest of the lemma follows.

□

By the construction of $M_1, ..., M_{16}$ in Lemma 3.2.7, we know the corresponding structure constants of $\mathrm{Mat}_4(K)$ from the structure constants of $\mathrm{Mat}_4(\bar{K})$ with the basis M'_P specified by $\xi_\epsilon \in (R \otimes R)^*$. It can also be checked that, given $M_1, ..., M_{16}$ with the derived structure constants, the matrices obtained via the change of basis specified by $\mathbf{P}^{-1}$ indeed satisfy the structure constants and Galois condition required for $\{M'_P, P \in J[2]\}$. Hence, to compute such M'_P for $P \in J[2]$, we first compute $M_1, ..., M_{16}$.

Description of the algorithm

Suppose $K = \mathbb{Q}$ and the genus two curve is defined by $y^2 = f(x)$. Let $L = \mathbb{Q}[x]/(f)$ and L_1 denote the splitting field of f. Now we give the naive method for computing a linear isomorphism $\psi_\epsilon : \mathcal{K}_\epsilon \subset\!\!\to \mathcal{K} \subset \mathbb{P}^3$ that corresponds to $\epsilon \in \mathrm{Sel}^2(J)$.

- Step 1: Compute $\xi \in (R \otimes R)^*$ such that $M_P M_Q = \xi(P, Q)M_{P+Q}$ for any $P, Q \in J[2]$, with the formulae for $\{M_P, P \in J[2]\}$ given in Lemma 3.2.1(ii).
- Step 2: For $\epsilon \in \mathrm{Sel}^2(J)$, compute its image in $L^*/(L^*)^2\mathbb{Q}^*$ via MAGMA as in Remark 3.2.8. Then compute $\rho \in (R \otimes R)^*$ as in Remark 3.2.4 and define $\xi_\epsilon = \rho \cdot \xi$.
- Step 3: From ξ_ϵ, we compute the structure constants for $\mathrm{Mat}_4(\mathbb{Q})$ with basis $M_1, ..., M_{16}$ defined in Lemma 3.2.7. Then we compute $M_1, ..., M_{16} \in \mathrm{Mat}_4(\mathbb{Q})$ explicitly via the algorithm in Section 3.4 and compute $\{M'_P, P \in J[2]\}$ via the change of basis specified by $\mathbf{P}^{-1}$ defined in Lemma 3.2.7.

- Step 4: Compute $A \in \mathrm{GL}_4(\bar{\mathbb{Q}})$ such that $AM'_P = M_P A \in \mathrm{PGL}_4(\bar{\mathbb{Q}})$, for all $P \in J[2]$. A result represents a linear isomorphism $\mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ corresponding to ϵ.

Remark 3.2.8. The existing algorithm for computing $\mathrm{Sel}^2(J)$, as implemented in MAGMA originally by Michael Stoll, represents Selmer group elements via their images in $L^*/(L^*)^2K^*$. Such computation in MAGMA is possible in the case where $K = \mathbb{Q}$ and in the case where f is degree 5 if K a general number field.

Remark 3.2.9. We can simplify Step 4 by picking generators P_1, P_2, P_3, P_4 for $J[2]$ and it suffices to solve for $A \in \mathrm{GL}_4(\bar{\mathbb{Q}})$ satisfying $AM'_{P_i} = M_{P_i}A \in \mathrm{PGL}_4(\bar{\mathbb{Q}})$, for all $i = 1, ..., 4$. More explicitly, we can pick $t_i \in \bar{\mathbb{Q}}$ such that $t_i^2 = \xi_\epsilon(P_i, P_i)/\xi(P_i, P_i)$ and solve for $A \in \mathrm{GL}_4(\bar{\mathbb{Q}})$ such that $AM'_{P_i} = t_i M_{P_i} A$, for all $i = 1, ..., 4$. Suppose the image of ϵ in $L^*/(L^*)^2\mathbb{Q}^*$ is represented by $\delta \in L^*$ which corresponds to $(a_1, a_2, ..., a_6)$ via evaluation at the 6 roots of f as discussed in Section 1.10.1. Solving the t_i is a linear algebra problem over $L_1(\sqrt{a_1}, \sqrt{a_2}, ..., \sqrt{a_6})$ which can be done by MAGMA. We observe that there are 16 choices of t_i, which is compatible with Lemma 3.2.2.

3.3 The Flex Algebra Method

Same as in Section 3.2, unless stated otherwise, we fix $\epsilon \in \mathrm{Sel}^2(J)$ and $(J_\epsilon, \pi_\epsilon)$ the 2-covering of J corresponding to ϵ. In this section, we will describe another method for explicitly computing a linear isomorphism $\psi_\epsilon : \mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ corresponding to ϵ. Recall, this means ψ_ϵ a linear change of coordinates on $\mathbb{P}^3$ in the commutative diagram of the base Brauer-Severi diagram $[J \to \mathbb{P}^3]$ and its twist $[J_\epsilon \to \mathbb{P}^3]$ that corresponds to ϵ and $\mathcal{K}_\epsilon = \psi_\epsilon^{-1}(\mathcal{K}) \subset \mathbb{P}^3$. So $\psi_\epsilon : \mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ and there exists an isomorphism $\phi_\epsilon : J_\epsilon \to J$ such that $[2] \circ \phi_\epsilon = \pi_\epsilon$, with a commutative diagram (1.6.2) in Remark 1.6.3 corresponding to ϵ. Equivalently, we look for a linear isomorphism $\psi_\epsilon : \mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ such that $(\sigma \mapsto \psi_\epsilon(\psi_\epsilon^{-1})^\sigma)$ gives a cocycle for ϵ. An advantage of this method, comparing to the native method, is that it requires a smaller field extension. Most results in this section generalize and follow the same proofs of the results in the elliptic curve case as in [CFO+08, Sections 4, 5].

3.3.1 Enveloping algebras

In this section, we give the definition of the enveloping algebra of a central extension of $J[2]$ by $\mathbb{G}_m$ and study its properties. It is a generalization of [CFO+08, Definition 4.1] and is needed when describing the flex algebra method in later sections.

Definition 3.3.1. Let Λ be a central extension of $J[2]$ by $\mathbb{G}_m$. Let A be a K-algebra with $[A:K]=16$. Denote $\bar{A}=A\otimes_K \bar{K}$. An *embedding* of $\mathbf{\Lambda}$ in A is a morphism of K-group varieties $\iota:\Lambda\to\bar{A}^*$ such that

(i) ι preserves scalars, i.e. $\iota(\lambda)=\lambda$ for all $\lambda\in\bar{K}^*$,

(ii) the image of ι spans $\bar{A}$ as a $\bar{K}$-vector space.

If Λ embeds in a K-algebra A, then we call A the *enveloping algebra* of Λ. Let $\mathbf{\Theta}$ be a theta group for $J[2]$. A special case of Definition 3.3.1 is when $\mathbf{\Theta}$ embeds in the matrix algebra $\mathrm{Mat}_4(K)$. An embedding in this case is a morphism of group varieties $\mathbf{\Theta}\to \mathrm{GL}_4$ that preserves scalars.

Remark 3.3.2. Recall that the base theta group $\mathbf{\Theta_J}$ is defined as a subgroup of GL_4. By Lemma 3.2.1(i), we get that $\mathbf{\Theta_J}$ naturally embeds in $\mathrm{Mat}_4(K)$. Similarly we constructed $\mathbf{\Theta}_\epsilon$ as a subgroup of GL_4 for $\epsilon\in \mathrm{Sel}^2(J)$ in Section 3.1.2, which is the twist of $\mathbf{\Theta_J}$ by ϵ shown in Lemma 3.1.7. We get $\mathbf{\Theta}_\epsilon$ also naturally embeds in $\mathrm{Mat}_4(K)$ as $\{M'_P, P\in J[2]\}$ is shown to be a basis for $\mathrm{Mat}_4(\bar{K})$ for $P\mapsto M'_P$ a section for $\mathbf{\Theta}_\epsilon\to J[2]$ in Section 3.2.1.

Before we state and prove results related to enveloping algebras, we first define the trace map $\mathrm{Tr}: R\otimes R\to R$, viewing $R\otimes R$ as an R-algebra via $\triangle: R\to R\otimes R$ where $\triangle(\rho)(P_1,P_2)=\rho(P_1+P_2)$. More explicitly, under the trace map, $\rho\in R\otimes R$ maps to

$$T\mapsto \sum_{T_1+T_2=T}\rho(T_1,T_2).$$

Recall $R\otimes R$ is the algebra of Galois equivariant maps from $J[2]\times J[2]$ in to $\bar{K}$. By Proposition 3.1.10, we know $R\otimes R$ is étale. The above map may also be built out of the trace maps for the constituent fields of $R\otimes R$ and R. We will prove it explicitly in a special case in Lemma 6.3.1.

Given an element $\rho\in(R\otimes R)^*$, we can define a new multiplication $*_\rho$ on R via

$$z_1 *_\rho z_2 := \mathrm{Tr}(\rho\cdot(z_1\otimes z_2)),$$

for $z_1, z_2\in R$.

The lemma below generalizes the results for elliptic curves as in [CFO+08, Lemma 4.5, Lemma 4.3]

Lemma 3.3.3. *The following statements hold.*

(i) Let Λ be a central extension of $J[2]$ by $\mathbb{G}_m$. Suppose $inv_2(\Lambda)=\rho\partial R^*$. Then Λ has enveloping algebra $(R,*_\rho)$.

(ii) Let Λ_1, Λ_2 be central extensions of $J[2]$ by $\mathbb{G}_m$ with enveloping algebras A_1, A_2. Then any isomorphism of central extensions $\psi : \Lambda_1 \to \Lambda_2$ extends uniquely to an isomorphism of K-algebras $\Psi : A_1 \to A_2$.

Proof. Define $\delta_P \in \bar{R}$ for $P \in J[2]$, such that $\delta_P(Q) = 1$ if $P = Q$ and $\delta_P(Q) = 0$ otherwise. This makes $\{\delta_P, P \in J[2]\}$ a basis for $\bar{R}$ as a $\bar{K}$-vector space. Now let $\phi : J[2] \to \Lambda$ be the Galois equivariant section for Λ such that $\phi(T_1)\phi(T_2) = \rho(T_1, T_2)\phi(T_1 + T_2)$. Consider the Galois equivariant inclusion of Λ in $\bar{R}$:

$$\lambda\phi(T) \mapsto \lambda\delta_T,$$

for all $\lambda \in \bar{K}^*$ and $T \in J[2]$. The group law on Λ extends uniquely to a new $\bar{K}$-algebra multiplication $*$ on $\bar{R}$, which then descends to a K-algebra multiplication $R \times R \to R$. In particular, we have

$$\delta_S * \delta_T = \rho(S, T)\delta_{S+T}.$$

for all $S, T \in J[2]$. Then

$$\begin{aligned} z_1 * z_2 &= (\sum_P z_1(P)\delta_P) * (\sum_P z_2(P)\delta_P) \\ &= \sum_P (\sum_{P_1+P_2=P} \rho(P_1, P_2) z_1(P_1) z_2(P_2))\delta_P \\ &= \mathrm{Tr}(\rho \cdot (z_1 \otimes z_2)). \end{aligned}$$

Hence, $* = *_\rho$ and Λ embeds in $(R, *_\rho)$ which gives (i).

For (ii), we construct Ψ by first extending ψ linearly to an isomorhism of $\bar{K}$-algebras and then restricting to K-algebras. By the definition of enveloping algebras, we know Ψ is unique.

□

Suppose the theta group $\mathbf{\Theta}$ has an embedding in $\mathrm{Mat}_4(K)$ and recall the discussion above Remark 3.3.2. Then by definition, we have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \mathbf{\Theta} & \longrightarrow & J[2] & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle =} & & \downarrow & & \downarrow{\scriptstyle \chi} & & \\ 0 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \mathrm{GL}_4 & \longrightarrow & \mathrm{PGL}_4 & \longrightarrow & 0. \end{array} \tag{3.3.1}$$

Moreover, we have the following corollary of Lemma 3.3.3.

Corollary 3.3.4. *Let $\mathbf{\Theta}$ be the twist of $\mathbf{\Theta_J}$ by $\epsilon \in Sel^2(J)$. Suppose $\mathbf{\Theta}$ has an embedding in $Mat_4(K)$ with a commutative diagram (3.3.1). There is a unique*

subvariety $\mathcal{K}_\epsilon \subset \mathbb{P}^3$ *that is the twisted Kummer surface corresponding to* ϵ *as in* (1.6.2) *with the action of* $P \in J[2]$ *on* $\mathcal{K}_\epsilon$ *given by* $\chi(P)$.

Proof. Fix $\mathcal{K}_\epsilon$ as a subvariety of $\mathbb{P}^3$. Recall we constructed $\mathbf{\Theta}_\epsilon$ which is a twist of $\mathbf{\Theta_J}$ by ϵ and consists of elements that represent the action of $J[2]$ on $\mathcal{K}_\epsilon \subset \mathbb{P}^3$. It has an embedding in $\mathrm{Mat}_4(K)$ as explained in Remark 3.3.2. By Proposition 3.1.6 and Lemma 3.3.3(ii), these two embeddings differ only by an automorphism of $\mathrm{Mat}_4(K)$. By the Noether Skolem theorem, this automorphism is conjugation by an element of $\mathrm{GL}_4(K)$. Hence, the existence part of the statement is proved via potentially a suitable change of coordinates on the ambient space of $\mathcal{K}_\epsilon \subset \mathbb{P}^3$. The uniqueness part follows from Lemma 3.2.2.

□

Suppose $\epsilon \in \mathrm{Sel}^2(J)$. We showed that the theta group $\mathbf{\Theta}_\epsilon$ naturally embeds in $\mathrm{Mat}_4(K)$ in Remark 3.3.2. Let $P \mapsto M'_P$ be a Galois equivariant section for $\mathbf{\Theta}_\epsilon \to J[2]$ such that $M'_P M'_Q = \xi_\epsilon M'_{P+Q}$, for $\xi_\epsilon \in (R \otimes R)^*$. By Lemma 3.3.3(i), we know $\mathrm{Mat}_4(K) \cong (R, *_{\xi_\epsilon})$. In fact, it can be checked that this isomorphism is given by $M'_P \mapsto \delta_P$ over $\bar{K}$. We verify

$$\begin{aligned}\delta_P *_{\xi_\epsilon} \delta_Q &= \mathrm{Tr}(\xi_\epsilon \delta_p \otimes \delta_Q) \\ &= \sum_{T \in J[2]} \sum_{P_1+P_2=T} \xi_\epsilon(P_1, P_2)\delta_P(P_1)\delta_Q(P_2)\delta_T \\ &= \xi_\epsilon(P, Q)\delta_{P+Q}.\end{aligned}$$

Let $r_1, ..., r_{16}$ be a basis for R and define $M_i = \sum_{P \in J[2]} r_i(p) M'_p$. Then we know $M_1, ..., M_{16}$ is a basis for $\mathrm{Mat}_4(K)$ as shown in Lemma 3.2.7. Hence, the isomorphism above restricts to an isomorphism $\mathrm{Mat}_4(K) \cong (R, *_{\xi_\epsilon})$ sending M_i to r_i defined over K.

3.3.2 Obstruction map and enveloping algebra

In this section, we introduce the definition of the obstruction map and explain how it is related to the enveloping algebra defined in the previous section.

Definition 3.3.5. The obstruction map

$$\mathrm{Ob} : H^1(G_K, J[2]) \to H^2(G_K, \bar{K}^*) \cong \mathrm{Br}(K)$$

is the composition of the map $H^1(G_K, J[2]) \to H^1(G_K, \mathrm{PGL}_4(\bar{K}))$ induced by the action of translation of $J[2]$ on $\mathbb{P}^3$ in the base Brauer-Severi diagram $J \xrightarrow{|2\Theta|} \mathbb{P}^3$, and the injective map $H^1(G_K, \mathrm{PGL}_4(\bar{K})) \to H^2(G_K, \bar{K}^*)$ induced from the short exact sequence $0 \to \bar{K}^* \to \mathrm{GL}_4(\bar{K}) \to \mathrm{PGL}_4(\bar{K}) \to 0$.

Remark 3.3.6. Suppose $[X \to S]$ is the Brauer-Severi diagram corresponding to $\epsilon \in H^1(G_K, J[2])$. Then there exist isomorphisms ϕ, ψ defined over $\bar{K}$ satisfying (1.6.1). In particular, $\phi(\phi^{-1})^\sigma = \tau_{\epsilon_\sigma}$ where $(\sigma \mapsto \epsilon_\sigma)$ is a cocycle representing ϵ. It follows that $\psi(\psi^{-1})^\sigma$ is the action of ϵ_σ on $\mathcal{K} \subset \mathbb{P}^3$ which implies that S is the twist of $\mathbb{P}^3$ corresponding to the image of ϵ in $H^1(G_K, \mathrm{PGL}_4)$. Hence, we can view $\mathrm{Ob}(\epsilon)$ as the Brauer-Severi variety S since $H^1(G_K, \mathrm{PGL}_4) \to \mathrm{Br}(K)$ is injective. Moreover, $\mathrm{Ob}(\epsilon)$ is trivial for $\epsilon \in \mathrm{Sel}^2(J)$ as the corresponding twisted Brauer-Severi diagram is $[J_\epsilon \to \mathbb{P}^3]$ by Lemma 1.6.2. The result for elliptic curves is in [CFO+08, Corollary 2.5].

Remark 3.3.7. In general the obstruction map is not a group homomorphism. But, as shown in [O'N02, Lemmas 4.2, 4.4], it is quadratic in the sense that

(i) $\mathrm{Ob}(a\epsilon) = a^2\mathrm{Ob}(\epsilon)$, for all $a \in \mathbb{Z}$, and
(ii) $(\epsilon, \eta) \mapsto \mathrm{Ob}(\epsilon + \eta) - \mathrm{Ob}(\epsilon) - \mathrm{Ob}(\eta)$ is bilinear.

We state and prove the proposition below on the relationship between the obstruction map and enveloping algebra. The result in the elliptic curve case is in [CFO+08, Theorem 4.10].

Proposition 3.3.8. *Let $\boldsymbol{\Theta}$ be a theta group for $J[2]$ with enveloping algebra A, then the obstruction map sends the class of $\boldsymbol{\Theta}$, considered as an element in $H^1(G_K, J[2])$, to the class of A in $Br(K)$.*

Proof. By Lemma 3.1.5, we know $\boldsymbol{\Theta}$ is a twist of $\boldsymbol{\Theta}_J$. Then by Lemma 3.3.3(ii) and Remark 3.3.2, we get that A is a twist of $\mathrm{Mat}_n(K)$ and hence a central simple K-algebra.

Suppose $\boldsymbol{\Theta}$ is a twist of $\boldsymbol{\Theta}_\mathbf{J}$ by $\epsilon \in H^1(G_K, J[2])$. By Proposition 1.5.3, we know that there exists an isomorphism $\gamma : \boldsymbol{\Theta} \to \boldsymbol{\Theta}_\mathbf{J}$ such that $\gamma(\gamma^{-1})^\sigma : x \mapsto e_2(\epsilon_\sigma, \beta_J(x))x$, for all $x \in \boldsymbol{\Theta}_\mathbf{J}$. Then by the commutator relationship, we know $\gamma(\gamma^{-1})^\sigma$ is conjugation by M_{ϵ_σ}. Since isomorphism between two theta groups extends uniquely to an isomorphism between their enveloping algebras by Lemma 3.3.3(ii), we get an isomorphism $\Gamma : \bar{A} \to \mathrm{Mat}_4(\bar{K})$ that extends γ. Hence, the image of ϵ via the map $H^1(G_K, J[2]) \to H^1(G_K, \mathrm{PGL}_4(\bar{K})) \cong H^1(G_K, \mathrm{Aut}(\mathrm{Mat}_4(\bar{K}))) \cong \{\text{isomorphism classes of twists of } \mathrm{Mat}_4(K)\}$ is the class of A. So, $\mathrm{Ob}(\epsilon) = [A]$ by Remark 1.4.14.

□

Suppose $\epsilon \in \mathrm{Sel}^2(J)$. We know the theta group $\boldsymbol{\Theta}_\epsilon$ is the twist of $\boldsymbol{\Theta}_\mathbf{J}$ corresponding to ϵ by Lemma 3.1.7 and it naturally embeds in $\mathrm{Mat}_4(K)$ as explained in Remark 3.3.2. Then the above proposition shows that $\mathrm{Ob}(\epsilon)$ is trivial which is compatible to the discussion in Remark 3.3.6.

3.3.3 Flex algebra

Recall that we have identified $H^1(G_K, J[2])$ with the isomorphism classes of 2-coverings of J, Brauer-Severi diagrams, commutative extensions of $J[2]$ by $\mathbb{G}_m$ and theta groups for $J[2]$. In this section, we show another interpretation of $H^1(G_K, J[2])$ before giving the definition of flex algebra.

Definition 3.3.9. A *J[2]-torsor* is a pair (Φ, μ), where Φ is a zero-dimensional variety and $\mu : J[2] \times \Phi \to \Phi$ is a morphism which induces a simple transitive action on the $\bar{K}$-points of Φ. An isomorphism of $J[2]$-torsors is an isomorphism between the varieties that respect the action of $J[2]$.

The trivial $J[2]$-torsor is $(J[2], +)$, with $+$ denoting the restriction of the group law on J. It can be checked that any $J[2]$-torsor, (Φ, μ), is a twist of the trivial torsor via the isomorphism $(J[2], +) \cong (\Phi, \mu)$ such that $P \mapsto \mu(P, P_0)$ for some fixed choice of $P_0 \in \Phi(\bar{K})$. We usually denote (Φ, μ) by Φ and we have the following parametrization of the isomorphism classes of $J[2]$-torsors.

Proposition 3.3.10. *The isomorphism classes of $J[2]$-torsors, viewed as twists of $(J[2], +)$, are parameterized by $H^1(G_K, J[2])$.*

Proof. Given a $J[2]$-torsor, (Φ, μ), the argument above shows that $P \mapsto \mu(P, P_0)$ for some fixed choice of $P_0 \in \Phi(\bar{K})$ defines the inverse of $\phi : (\Phi, \mu) \cong (J[2], +)$. It can be checked that $\phi(\phi^{-1})^\sigma$ is a translation by some $P_\epsilon \in J[2]$ and $(\sigma \mapsto P_\epsilon)$ is a cocycle in $Z^1(G_K, J[2])$. On the other hand, suppose $\epsilon \in H^1(G_K, J[2])$ has cocycle representation $(\sigma \mapsto \epsilon_\sigma)$. There exists a 2-covering of J, $(J_\epsilon, [2] \circ \phi_\epsilon)$, such that $\phi_\epsilon(\phi_\epsilon^{-1})^\sigma = \tau_{\epsilon_\sigma}$ by Proposition 1.5.10. From Proposition 1.5.7, we know $\mu : (P, Q) \mapsto \phi_\epsilon^{-1}(P + \phi_\epsilon(Q))$ is a simply transitive action of J on J_ϵ defined over K. Hence, this restricts to a simply transitive action of $J[2]$ on $\phi_\epsilon^{-1}(J[2])$ defined over K which makes $\phi_\epsilon^{-1}(J[2])$ a $J[2]$-torsor that gives rise to the cocycle $(\sigma \mapsto \epsilon_\epsilon)$. The rest of the proof is following routine arguments, as in Propositions 1.5.10 and 1.6.1.

□

Remark 3.3.11. Let $(J_\epsilon, \pi_\epsilon)$ be the 2-covering of J that corresponds to $\epsilon \in H^1(G_K, J[2])$. Suppose $[2] \circ \phi_\epsilon = \pi_\epsilon$. We know $\pi_\epsilon^{-1}(\mathcal{O}_J) = \phi_\epsilon^{-1}(J[2])$ is a $J[2]$-torsor corresponding to ϵ by the proof of Proposition 3.3.10. In the case where $\epsilon \in \mathrm{Sel}^2(J)$, we have the twisted Kummer $\mathcal{K}_\epsilon \subset \mathbb{P}^3$ and we can also view the singular points on $\mathcal{K}_\epsilon$ as a $J[2]$-torsor corresponding to ϵ.

Definition 3.3.12. Let $\epsilon \in H^1(G_K, J[2])$. The flex algebra of ϵ is the enveloping algebra of the commutative extension of $J[2]$ by $\mathbb{G}_m$ that corresponds to ϵ.

We show the following lemma, where the result in the elliptic curve case is in [CFO+08, Theorem 4.8].

Lemma 3.3.13. *Let $\epsilon \in H^1(G_K, J[2])$ and let Φ denote the $J[2]$-torsor that corresponds to ϵ. The flex algebra of ϵ is isomorphic to the étale algebra of Φ.*

Proof. Let F denote the étale algebra of Φ, which means $F = \mathrm{Map}_K(\Phi, \bar{K})$. define

$$\begin{aligned}\Lambda =&\{z \in \bar{F}^* : \text{ there exists } T \in J[2] \text{ such that } z(S+P) = e_2(S,T)z(P) \text{ for all} \\ & S \in J[2], P \in \Phi\}.\end{aligned}$$

By the non-degeneracy of the Weil pairing, we obtain a commutative extension of $J[2]$ by $\mathbb{G}_m$:

$$0 \mapsto \mathbb{G}_m \xrightarrow{\alpha} \Lambda \xrightarrow{\beta} J[2] \mapsto 0,$$

where $\beta(z) = T$ using the notation in the definition of Λ.

It suffices to show the Λ constructed from Φ is the commutative extension of $J[2]$ by $\mathbb{G}_m$ corresponding to ϵ, as Λ embeds in F by construction. Consider the isomorphism $\psi : \Phi \to J[2]$ such that $\psi(\psi^{-1})^\sigma = \tau_{\epsilon_\sigma}$ with the cocycle $(\sigma \mapsto \epsilon_\sigma)$ representing ϵ. This isomorphism ψ induces an isomorphism $\bar{F} = \mathrm{Map}(\Phi, \bar{K}) \to \bar{R} = \mathrm{Map}(J[2], \bar{K})$:

$$z \mapsto (P \mapsto z(\psi^{-1}(P))).$$

It can be checked that this then restricts to an isomorphism between the central extensions $\Psi : \Lambda \to \Lambda_0$, where $\Lambda_0 = \mathrm{G}_m \times J[2] = \{\lambda w(T) \in \bar{R}^* : \lambda \in \bar{K}^*, T \in J[2]\}$. Then, viewing $\Lambda_0 = \{\lambda w(T) \in \bar{R}^* : \lambda \in \bar{K}^*, T \in J[2]\}$, we have

$$\Psi(\Psi^{-1})^\sigma : z \mapsto \Psi(z \circ \psi^\sigma) = z \circ \tau_{\epsilon_\sigma}.$$

It can be checked that, viewing $\Lambda_0 = \mathrm{G}_m \times J[2]$, we have

$$\Psi(\Psi^{-1})^\sigma : x \mapsto e_2(\epsilon_\sigma, x)x,$$

as required.

□

Remark 3.3.14. The proof of Lemma 3.3.13 shows the compatibility between the parameterization of the isomorphism classes of $J[2]$-torsors and the parameterization of the isomorphism classes of commutative extensions of $J[2]$ by $\mathbb{G}_m$ by $H^1(G_K, J[2])$. Let $\epsilon \in \mathrm{Sel}^2(J)$ and suppose $w_2(\epsilon) = \rho\partial R^*$. By Lemmas 3.1.15 and 3.3.3(i), we know that the flex algebra of ϵ is $(R, *_\rho)$. Then by Lemma 3.3.13, we have $(R, *_\rho) \cong F = \mathrm{Map}_K(\Phi, \bar{K})$, where Φ denotes the $J[2]$-torsor

that corresponds to ϵ.

Recall that we always embed $\mathcal{K} \subset \mathbb{P}^3$ as in Section 1.3.2 and we have explicit formulae for $\{M_P \in \mathrm{GL}_4(\bar{K}), P \in J[2]\}$ representing the action of $J[2]$ on $\mathcal{K} \subset \mathbb{P}^3$ given in Lemma 3.2.1(ii). In particular $P \mapsto M_P$ is Galois equivariant. Define $M \in \mathrm{GL}_4(R) = \mathrm{Map}_K(J[2], \mathrm{GL}_4(\bar{K}))$ such that $M(P) = M_P$, for $P \in J[2]$. We also define $\xi \in (R \otimes R)^*$ such that $M_P M_Q = \xi(P,Q) M_{P+Q}$ for all $P, Q \in J[2]$. Suppose $w_2(\epsilon) = \rho \partial R^*$ for $\rho \in (R \otimes R)^*$. Let $\xi_\epsilon = \rho\xi$. By Lemma 3.3.3(i) and Lemma 3.1.16, $A = (R, *_\xi)$ and $A_\epsilon = (R, *_{\xi_\epsilon})$ are the enveloping algebras for $\mathbf{\Theta_J}$ and the theta group corresponding to ϵ. Since $\epsilon \in \mathrm{Sel}^2(J)$, we showed in Section 3.3.1 that $(A, *_{\xi_\epsilon}) \cong \mathrm{Mat}_4(K)$. We now prove two propositions following the proofs in the elliptic curve case as in [CFO+08, Theorems 5.8, 5,9].

Proposition 3.3.15. *Let $\epsilon \in Sel^2(J)$. Suppose $w_2(\epsilon) = \rho \partial R^*$ for $\rho \in (R \otimes R)^*$. Let $\xi_\epsilon = \rho\xi$. Define $A = (R, *_\xi)$ and $A_\epsilon = (R, *_{\xi_\epsilon})$.*

(i) Suppose we have $\gamma \in \bar{R}^*$ such that $\partial\gamma = \rho$, then there exists an isomorphism of $\bar{K}$-algebras $\cdot\gamma : \bar{A}_\epsilon \to \bar{A}$. Note the multiplication is that in R.

(ii) Suppose we have $\gamma \in \bar{R}^*$ such that $\cdot\gamma : \bar{A}_\epsilon \to \bar{A}$ is an isomorphism of $\bar{K}$-algebras. For any isomorphism $\tau_\epsilon : A_\epsilon \cong Mat_4(K)$ as K-algebras and the isomorphism of K-algebras $\tau : A \to Mat_n(K)$ given by $\tau(x)_{ij} = tr_{R/K}(xM_{ij}) = \sum_{P \in J[2]}(x(P)(M_P)_{ij})$, we have the following commutative diagram:

$$\begin{array}{ccc} \bar{A}_\epsilon & \xrightarrow{\tau_\epsilon} & Mat_4(\bar{K}) \\ \downarrow{\scriptstyle \cdot\gamma} & & \downarrow{\scriptstyle \beta} \\ \bar{A} & \xrightarrow{\tau} & Mat_4(\bar{K}), \end{array} \tag{3.3.2}$$

where β is the conjugation by a matrix $B \in GL_4(\bar{K})$ which represents a change of coordinates on $\mathbb{P}^3$ in the commutative diagram of the base Brauer-Severi diagram $[J \to \mathbb{P}^3]$ and its twist $[J_\epsilon \to \mathbb{P}^3]$ that corresponds to the Selmer element ϵ.

Proof. We note that A and A_ϵ are central simple algebras of the same dimension. Hence, to show a map is an isomorphism, it suffices to show that it is a ring homomorphism. For (i), we have that $\gamma \cdot (z_1 *_{\xi_\epsilon} z_2)$ sends $T \in J[2]$ to

$$\begin{aligned} &\gamma(T) \sum_{T_1+T_2=T} \xi_\epsilon(T_1, T_2) z_1(T_1) z_2(T_2) \\ &= \sum_{T_1+T_2=T} \xi(T_1, T_2) \gamma(T_1) z_1(T_1) \gamma(T_2) z_2(T_2), \end{aligned}$$

which is $(\gamma \cdot z_1) *_\xi (\gamma \cdot z_2)$ as required.

For (ii), we first need to show that τ is a ring homomorphism. It suffices to prove it over $\bar{K}$, where $\tau(\delta_P) = M_P$. Since $\delta_P *_\xi \delta_Q = \xi(P,Q)\delta_{P+Q}$ and $M_P M_Q = \xi(P,Q)M_{P+Q}$, the result follows.

Then for the remaining part of the proposition, we let β be the isomorphism that makes (3.3.2) commute. By the Noether Skolem theorem, we have that β is conjugation by some matrix $B \in \mathrm{GL}_4(\bar{K})$. Since A, A_ϵ are the enveloping algebras of $\mathbf{\Theta_J}$ and $\mathbf{\Theta}$, the twist of $\mathbf{\Theta_J}$ by ϵ, we now get embeddings of $\mathbf{\Theta_J}$ and $\mathbf{\Theta}$ in $\mathrm{Mat}_4(K)$ via composing with the isomorphisms τ, τ_ϵ respectively. In this way, $\mathbf{\Theta_J}$ and $\mathbf{\Theta}$ are now subgroups of GL_4 generated up to scalars by $\tau(\delta_P)$ ad $\tau_\epsilon(\delta_P)$ for $P \in J[2]$. We observe that $\tau(P) = M_P$ for any $P \in J[2]$. The commutativity of (3.3.2) shows that $\mathbf{\Theta_J} \subset \mathrm{GL}_4$ and $\mathbf{\Theta} \subset \mathrm{GL}_4$ are related by conjugation by B. By Corollary 3.3.4, we know there exists a unique subvariety $\mathcal{K}_\epsilon \subset \mathbb{P}^3$ that is the twisted Kummer corresponding to ϵ as in (1.6.1) such that $\mathbf{\Theta}$ consists of elements that represent the action of $J[2]$ on $\mathcal{K}_\epsilon$. This implies that there exists $C \in \mathrm{GL}_4(\bar{K})$ such that $\mathbf{\Theta_J} \subset \mathrm{GL}_4$ and $\mathbf{\Theta} \subset \mathrm{GL}_4$ are related by conjugation by C. Hence, BC^{-1} represents an element in $\mathrm{PGL}_4(\bar{K})$ that commutes with M_P in $\mathrm{PGL}_4(\bar{K})$ for all $P \in J[2]$ which implies the induced isomorphism $BC^{-1} = M_Q \in \mathrm{PGL}_4(\bar{K})$ for some $Q \in J[2]$ by Lemma 3.2.1(i). Therefore, B represents the change of coordinates on $\mathbb{P}^3$ in the commutative diagram of the base Brauer-Severi diagram and its twist $[J_\epsilon \to \mathcal{K}_\epsilon \subset \mathbb{P}^3]$ corresponding to ϵ.

□

We now modify the above method for computing the twist of Kummer $\mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$. Proposition 3.3.15 suggests that we need to solve for $\gamma \in (R \otimes \bar{K})^*$ such that $\partial\gamma = \rho$. Recall in Remark 3.3.11, we showed $\Phi = \pi_\epsilon^{-1}(\mathcal{O}_J)$ is a $J[2]$-torsor induced by the 2-covering $(J_\epsilon, \pi_\epsilon)$ of J corresponding to ϵ. The next proposition shows that we can actually solve for $\gamma \in (R \otimes F_1)^*$ where F_1 is the field of definition of a point in Φ. We follow the proof of the result in the elliptic curve case in [CFO+08, Theorem 5.9].

Proposition 3.3.16. *Let $\epsilon \in Sel^2(J)$. Suppose $w_2(\epsilon) = \rho\partial R^*$ for $\rho \in (R \otimes R)^*$. Let $\xi_\epsilon = \rho\xi$. Define $A = (R, *_\xi)$, $A_\epsilon = (R, *_{\xi_\epsilon})$ and $F = (R, *_\rho)$.*

(i) We have an isomorphism of F-algebras $\alpha : A_\epsilon \otimes_K F \to A \otimes_K F$ such that

$$x \otimes 1 \mapsto \sum_{i=1}^{n^2} r_i^* x \otimes r_i,$$

where $r_1, .., r_{16}$ is a set of basis for R and $r_1^*, ..., r_{16}^*$ is its dual basis with respect to the trace form $(r,s) \mapsto tr_{R/K}(rs) = \sum_{P \in J[2]} r(P)s(P)$, i.e. $(r_i^*, r_j) = \delta_{ij}$.

(ii) We have the following commutative diagram with τ, τ_ϵ defined in Proposition 3.3.15:

$$\begin{array}{ccc} A_\epsilon \otimes F & \xrightarrow{\tau_\epsilon} & Mat_4(F) \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} \\ A \otimes F & \xrightarrow{\tau} & Mat_4(F), \end{array}$$

where β is conjugation by some matrix $B \in GL_4(F) = Map_K(\Phi, GL_4(\bar{K}))$ with Φ a $J[2]$-torsor corresponding to ϵ. Moreover, for each $Q \in \Phi$, the matrix $B_Q \in GL_4(\bar{K})$ represents a change of coordinates on $\mathbb{P}^3$ in the commutative diagram of the Brauer-Severi diagram $[J \to \mathbb{P}^3]$ and its twist $[J_\epsilon \to \mathbb{P}^3]$ that corresponds to the Selmer element ϵ.

Proof. We observe that α is multiplication by $\Gamma = (1 \otimes \iota_F)(\sum_{i=1}^{16} r_i^* \otimes r_i) \in R \otimes F$ where $\iota_F : R \cong F$ is the isomorphism of the underlying K-vector space and it can be checked that the definition of α is independent of the choice of basis $r_1, ..., r_{16}$. To show α a ring homomorphism, it suffices to prove it over $\bar{K}$ and assume $r_i = \delta_{P_i} = r_i^*$, where $P_1, ..., P_{16}$ are the 16 points in $J[2]$. Hence, we need

$$\sum_{i=1}^{16} \delta_{P_i}(\delta_S *_{\xi_\epsilon} \delta_T) \otimes \delta_{P_i} = \sum_{i=1}^{16}\sum_{j=1}^{16} (\delta_{P_i}\delta_S *_\xi \delta_{P_j}\delta_T) \otimes (\delta_{P_i} *_\rho \delta_{P_j}).$$

With some simplification, the above equation becomes

$$\xi(S,T)\rho(S,T)\delta_{S+T} \otimes \delta_{S+T} = \xi(S,T)\delta_{S+T} \otimes \rho(S,T)\delta_{S+T},$$

which always holds. Then, it can be checked that α is indeed an isomorphism which gives (i).

For (ii), we define β to be the isomorphism of F-algebras that makes the above diagram commute. Since F is the flex algebra of ϵ, by Remark 3.3.14, we know it is the étale algebra of Φ which implies it is a product of field extensions of K. Hence, β is conjugation by some matrix $B \in \mathrm{GL}_4(F)$ via applying the Noether Skolem theorem to each constituent field of F. We note α is multiplication by $\Gamma = (1 \otimes \iota_F)(\sum_{i=1}^{16} r_i^* \otimes r_i) \in R \otimes F$ at the start of the proof. This implies that for each $Q \in \Phi$, we get the commutative diagram (3.3.2) with γ replaced with $\Gamma_Q \in \bar{R}^*$ and β is conjugation by $B_Q \in \mathrm{GL}_n(\bar{K})$. Then the result follows by Proposition 3.3.15.

□

Remark 3.3.17. Follow the notation in the above two propositions. We observe that any ring homomorphism $\bar{A}_\epsilon \xrightarrow{\cdot\gamma} \bar{A}$ for some $\gamma \in \bar{R}^*$ satisfies $\partial\gamma = \rho$. Indeed, we have $\gamma\delta_S *_\xi \gamma\delta_T = \gamma\delta_S *_{\xi_\epsilon} \delta_T$ which simplifies to $\gamma(S)\gamma(T) = \gamma(S+T)\rho(S,T)$ for any $S, T \in J[2]$. This then implies that $\bar{A}_\epsilon \xrightarrow{\cdot\gamma} \bar{A}$ for some $\gamma \in \bar{R}^*$ is a ring

homomorphism if and only if $\partial\gamma = \rho$ by Proposition 3.3.15(i). Note such ring homomorphism is an isomorphism as A_ϵ is central simple. Since $w_2(\epsilon) = \rho\partial R^*$, we know there exists $\gamma_0 \in \bar{R}^*$ such that $w(\epsilon_\sigma) = \sigma(\gamma_0)/\gamma_0$ and $\partial\gamma_0 = \rho$ where $(\sigma \mapsto \epsilon_\sigma)$ is a cocycle representation of ϵ. Via the exactness of (3.1.1), we know each Γ_Q constructed in Proposition 3.3.16 is $\gamma_0 w(P)$ for some $P \in J[2]$. Moreover, since $r_1, ..., r_{16}$ is a basis for R, we know $\Gamma_{Q_1} \neq \Gamma_{Q_2}$ for $Q_1 \neq Q_2 \in \Phi$. Hence, we have $\{\Gamma_Q, Q \in \Phi\} = \{\gamma_0 w(P), P \in J[2]\}$.

3.3.4 Algorithm for the flex algebra method

In this section, we describe the flex algebra method for computing the linear isomorphism $\mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ corresponding to $\epsilon \in \mathrm{Sel}^2(J)$. Here, we assume $K = \mathbb{Q}$ and we have an algorithm that trivializes a matrix algebra specified by its structure constants.

- Step 1: Compute $\xi \in (R \otimes R)^*$ such that $M_P M_Q = \xi(P, Q) M_{P+Q}$ for any $P, Q \in J[2]$, with the formulae for $\{M_P, P \in J[2]\}$ given in Lemma 3.2.1(ii).

- Step 2: For $\epsilon \in \mathrm{Sel}^2(J)$, compute its image in $L^*/(L^*)^2\mathbb{Q}^*$ via MAGMA and recall Remark 3.2.8. Then compute $\rho \in (R \otimes R)^*$ as in Remark 3.2.4 and define $\xi_\epsilon = \rho \cdot \xi$.

- Step 3: Let $A = (R, *_\xi)$. As specified in Proposition 3.3.15, we compute the isomorphism $\tau : A \to \mathrm{Mat}_4(\mathbb{Q})$.

- Step 4: Let $A_\epsilon = (R, *_{\xi_\epsilon})$. Compute the structure constants of A_ϵ with respect to a basis of R and use the algorithm in Section 3.4 to compute an isomorphism $\tau_\epsilon : A_\epsilon \to \mathrm{Mat}_4(\mathbb{Q})$.

- Step 5: Let $F = (R, *_\rho)$. Compute the following composition of maps:

$$\tau'_\epsilon : A_\epsilon \xrightarrow{\alpha} A \otimes F \xrightarrow{\tau} \mathrm{Mat}_4(F),$$

  which is given by $x \mapsto \sum_{i=1}^{16} \tau(r_i^* x) \otimes r_i$ with details explained in Proposition 3.3.16.

- Step 6: Solve for a matrix $B \in \mathrm{GL}_4(F)$ such that $B\tau_\epsilon(x) = \tau'_\epsilon(x)B$ for all $x \in R$. This is a linear algebra problem over F, where $[F : \mathbb{Q}] = 16$ and can be solved using MAGMA.

The flex algebra method for computing the explicit twist map of $\mathcal{K}$ requires a much smaller number field than the naive method in general. In Chapter 6, we will give more details on the computation using the flex algebra in a special case.

3.4 Trivializing Matrix Algebras over $\mathbb{Q}$

Recall that in Sections 3.2 and 3.3, we gave two methods for computing a linear isomorphism $\mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ for $\epsilon \in \mathrm{Sel}^2(J)$. In the description of these methods, we required an algorithm that trivializes a $\mathbb{Q}$-algebra that is known to be isomorphic to $\mathrm{Mat}_4(\mathbb{Q})$ and specified by its structure constants. More precisely, we need to solve Problem 3.4.1 in the case $n = 4$. The algorithm we give in this section works in principle over any number field K. However, it is more practical over the field of rationals. Hence, in this section we assume $K = \mathbb{Q}$. A similar algorithm for trivializing an algebra $A \cong \mathrm{Mat}_n(\mathbb{Q})$ is done in [CFO+15, Section 6]. However, there it was mostly under the assumption that n is prime, which does not apply to our case. Hence, we also need to combine with the results done in [Pil07] to complete the algorithm for the case $n = 4$. We will discuss the details in this section. Also, see [IRS12] for the algorithm and complexity analysis in the general case.

Problem 3.4.1. Given a $\mathbb{Q}$-algebra A that we know is isomorphic to $\mathrm{Mat}_n(\mathbb{Q})$, compute the isomorphism explicitly. More precisely, we need to find a practical algorithm for the following:

The input of the algorithm is a list of structure constants $c_{ijk} \in \mathbb{Q}$ corresponding to a set of basis $a_1, ..., a_{n^2}$ of A such that $a_i a_j = \sum_{i,j} c_{ijk} a_k$. The return of the algorithm is $M_1, ..., M_{n^2}$, a set of basis for $\mathrm{Mat}_n(\mathbb{Q})$ such that

$$M_i M_j = \sum_{i,j} c_{ijk} M_k.$$

Note that the output is not unique since conjugating the basis elements M_i by any matrix in $\mathrm{GL}_n(\mathbb{Q})$ also works.

3.4.1 Subproblem: case n=2

It will be shown that a subproblem of Problem 3.4.1 in the case $n = 4$ is Problem 3.4.1 in the case $n = 2$. Finding such an isomorphism over $\mathbb{Q}$ is equivalent to finding a rational point on a plane conic. There exist algorithms for solving this, see for example [CR03][IS96][Sim05]. Here, we give one method for finding the explicit isomorphism and the results also hold if $K = \mathbb{R}$.

Lemma 3.4.2. *The quaternion algebras (a, b) and (a, c) are isomorphic if and only if bc is a norm in the extension $K(\sqrt{a})/K$. Moreover, finding the explicit isomorphism is equivalent to solving the conic $ax^2 + bcy^2 = z^2$ in the case a is not a square.*

Proof. Since the class of a quaternion algebra is in Br[2], we know $(a,b) \cong (a,c)$ if and only if $(a,b)+(a,c) = 0$. By Proposition 1.4.11(ii), we then know $(a,b) \cong (a,c)$ if and only if $(a,bc) = 0$ which by Proposition 1.4.11(iii) is if and only if bc is a norm in the extension of $K(\sqrt{a})/K$.

Now as for the explicit isomorphism, we have the following.

Let $1,i,j,ij$ denote the basis for (a,b) and $1,i,k,ik$ be the basis of (a,c). Then we have $i^2 = a, j^2 = b, ij = -ji$ and need to find $r,s,t,u \in K$ such that $k = r + si + tj + uij$ satisfying $k^2 = c$ and $ik = -ki$.

Some calculations show that we need $r = s = 0$ and $c = (t+ui)(t-ui)b$. Suppose a is not a square in K, then we have

$$bc = N_{K(\sqrt{a})/K}((t+u\sqrt{a})b).$$

This implies that finding $t,u \in K$ and hence the explicit isomorphism is equivalent to solving the norm equation of bc over the extension $K(\sqrt{a})/K$ which is also equivalent to solving the conic $ax^2 + bcy^2 = z^2$. Notice that since a is not a square, a solution to the conic has $y \neq 0$. Let (x_0,y_0,z_0) be a solution to the conic, then $bc = N_{K(\sqrt{a})/K}(\frac{z_0}{y_0} + \frac{x_0}{y_0}\sqrt{a})$. Hence $k = \frac{z_0}{y_0 b}j + \frac{x_0}{y_0 b}ij$ works, which gives the isomorphism required.

□

Remark 3.4.3. Suppose the quaternion algebras (a,b) and (a,c) are isomorphic and a is a square in K. We can assume $a = 1$ and let $1,i,j,ij$ denote the basis for (a,b). Then define $k = \frac{c+b}{2b}j + \frac{c-b}{2b}ij$ and we get that $1,i,k,ik$ is a basis for (a,c).

Corollary 3.4.4. *Given a K-algebra A that is known to be isomorphic to $Mat_2(K)$, there is a practical algorithm that finds such isomorphism explicitly.*

Proof. Using the algorithm as described in [Voi05, Algorithm 4.2.9], we can find an explicit isomorphism between A and some quaternion algebra (a,b). Note that this algorithm has already been implemented in MAGMA. We know $(a,b) \cong (1,1)$. If a or b is a square, then we get an isomorphism between $(1,1)$ and (a,b) following Remark 3.4.3. Else, we first get an explicit isomorphism between $(1,1)$ and $(a,1)$ then we find an explicit isomorphism between (a,b) and $(a,1)$ following the proof of Lemma 3.4.2. This gives us the explicit isomorphism between (a,b) and $(1,1)$. We then have an explicit isomorphism between (a,b) and $\mathrm{Mat}_2(K)$ via taking the generators of $(1,1)$ to be $\begin{bmatrix} 1,0 \\ 0,-1 \end{bmatrix}$ and $\begin{bmatrix} 0,1 \\ 1,0 \end{bmatrix}$ in $\mathrm{Mat}_2(K)$.

□

Remark 3.4.5. Suppose we have an explicit isomorphism $\phi : A \to \mathrm{Mat}_2(K)$. Then ϕ^{-1} maps $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ to a nonzero zero divisor of A.

3.4.2 Trivializing the algebra given a zero divisor

Corollary 3.4.4 describes a practical solution to Problem 3.4.1 in the case $n = 2$. Now our goal is to solve Problem 3.4.1 in the case $n = 4$. One approach requires first trivializing the algebra over $\mathbb{R}$. Let A be a K-algebra that we know is isomorphic to $\mathrm{Mat}_4(K)$, here K can be $\mathbb{Q}$ or $\mathbb{R}$. In this section, we give an algorithm that constructs an explicit isomorphism $A \cong \mathrm{Mat}_4(K)$ given a nonzero zero divisor $d \in A$ as done in [Pil07]. First we have the following lemma.

Lemma 3.4.6. *Let A_1 be a left A-module of dimension 4 with a fixed choice of basis. We define $\phi : A \to Mat_4(K) \cong End(A_1)$ that sends $a \in A$ to the matrix representing the endomorphism $x \mapsto ax$ on A_1 as a vector space. Then ϕ is an isomorphism of algebras.*

Proof. We observe ϕ is a nontrivial ring homomorphism. Since A is an simple algebra, ϕ is injective which implies that it is an isomorphism by a dimension check.

□

Define $\rho_d : A \to A$ a homomorphism of left A-modules with $\rho_d(a) = ad$. We have the following lemma using the Jordan Normal Form. In the case $K = \mathbb{Q}$, the result is stated and proved in [Pil07, Lemma 5]. It is clear from the proof that the same result holds over any field.

Lemma 3.4.7. *Let $\phi : A \to Mat_4(K)$ be an isomorphism and let $d \in A$ be a nonzero zero divisor such that none of $\ker \rho_d, \mathrm{Im}\, \rho_d, \ker \rho_d \cap \mathrm{Im}\, \rho_d$ has dimension 4. Then $\phi(d)$ is similar to one of the following block matrices:*

(1) $\begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix}$, *where $D \in Mat_2(K)$ is an invertible matrix;*

(2) $\begin{bmatrix} B & 0 \\ 0 & B \end{bmatrix}$, *where B is the matrix* $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$.

Remark 3.4.8. Suppose $d \in A$ is a nonzero zero divisor and $\phi : A \to \mathrm{Mat}_4(K)$ is an isomorphism. We check that $\phi(d)$ similar to a block matrix of type (1) in Lemma 3.4.7 implies that $\dim \mathrm{Im}\, \rho_d = 8$ and $\dim(\ker \rho_d \cap \mathrm{Im}\, \rho_d) = 0$. Similarly, $\phi(d)$ similar to a block matrix of type (2) in Lemma 3.4.7 implies that $\dim \mathrm{Im}\, \rho_d = 8$ and $\dim(\ker \rho_d \cap \mathrm{Im}\, \rho_d) = 8$.

Suppose we have a nonzero zero divisor $d \in A$. We know that the rank of d is 1, 2, or 3, corresponding to $\dim \operatorname{Im} \rho_d$ being 4, 8, 12 respectively. We then have the following cases.

- Case 1: $\dim \operatorname{Im} \rho_d = 4$. Then applying Lemma 3.4.6 with $A_1 = \operatorname{Im} \rho_d$ gives an isomorphism $A \cong \mathrm{Mat}_4(K)$.
- Case 2: $\dim \operatorname{Im} \rho_d = 12$. This implies $\dim \ker \rho_d = 4$. Then applying Lemma 3.4.6 with $A_1 = \ker \rho_d$ gives an isomorphism $A \cong \mathrm{Mat}_4(K)$.
- Case 3(i): $\dim \operatorname{Im} \rho_d = 8$ and $\dim(\ker \rho_d \cap \operatorname{Im} \rho_d) = 4$. Then applying Lemma 3.4.6 with $A_1 = \ker \rho_d \cap \operatorname{Im} \rho_d$ gives an isomorphism $A \cong \mathrm{Mat}_4(K)$.
- Case 3(ii): $\dim \operatorname{Im} \rho_d = 8$ and $\dim(\ker \rho_d \cap \operatorname{Im} \rho_d) = 0$. Let $\phi : A \to \mathrm{Mat}_4(K)$ be an isomorphism. From Lemma 3.4.7 and Remark 3.4.8, we know $\phi(d)$ is similar to a block matrix of type (1) in Lemma 3.4.7.

  Now define $\lambda_d : A \mapsto A$ with $\lambda_d(a) = da$. It can be directly checked that in this case the intersection $A_1 = \operatorname{Im} \rho_d \cap \operatorname{Im} \lambda_d$ is mapped by ϕ to the sub-algebra of all matrices with only the upper left 2 by 2 sub-matrix being possibly nonzero. So $A_1 \cong \mathrm{Mat}_2(K)$. Let d_1 be nonzero zero divisor in A_1, which can be explicitly found via Corollary 3.4.4 and Remark 3.4.5. This implies that d_1 is rank 1 in A_1 and hence it is also rank 1 in A. Now applying Case 1 with d_1 gives the trivialization required.
- Case 3(iii): $\dim \operatorname{Im} \rho_d = 8$ and $\dim(\ker \rho_d \cap R_d) = 8$. Let $\phi : A \to \mathrm{Mat}_4(K)$ be an isomorphism. From Lemma 3.4.7 and Remark 3.4.8, we know $\phi(d)$ is similar to matrix $\begin{bmatrix} B & 0 \\ 0 & B \end{bmatrix}$, where B is the matrix $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$.

  In this case, we let A_d denote the centralizer $C_A(d)$ and $\mathcal{R}(A_d)$ denote $\ker \rho_d \cap \ker \lambda_d$. Then there is the natural projection $\pi : A_d \mapsto A_d/\mathcal{R}(A_d)$. The following Lemma is needed and the result in the case $K = \mathbb{Q}$ is in [Pil07, Lemma 6]. We note that the proof in [Pil07, Lemma 6] works over any field, and we include it here as we need to follow it in the algorithm.

Lemma 3.4.9. *The algebra $\pi(A_d)$ is isomorphic to $Mat_2(K)$. If $e \in \pi(A_d)$ is a nonzero zero divisor, then for a generic element f in $\pi^{-1}(e)$ we have* $\dim \ker \rho_f = 4$.

(Note, here a "generic element" means an element in a dense Zariski open subset.)

Proof. We may assume $\phi(d)$ is actually equal to $\begin{bmatrix} B & 0 \\ 0 & B \end{bmatrix}$, where B is the matrix $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$. Then it can be checked that

$$\phi(A_d) = \{ \begin{bmatrix} \alpha_1 & \beta_1 & \alpha_2 & \beta_2 \\ 0 & \alpha_1 & 0 & \alpha_2 \\ \alpha_3 & \beta_3 & \alpha_4 & \beta_4 \\ 0 & \alpha_3 & 0 & \alpha_4 \end{bmatrix} : \alpha_i, \beta_i \in K \}.$$

We compute that $\phi(\mathcal{R}(A_d)) \subset \phi(A_d)$ consists of all elements in $\phi(A_d)$ such that $\alpha_i = 0$, for all i. This implies that $\phi(A_d)/\phi(\mathcal{R}(A_d)) \cong \{a \in \phi(A_d) : \beta_i = 0, \text{ for all } i\}$, which can be checked to be isomorphic to $\mathrm{Mat}_2(K)$.

Now consider the natural projection $\pi' : \phi(A_d) \mapsto \phi(A_d)/\phi(\mathcal{R}(A_d)) \cong \mathrm{Mat}_2(K)$. If e is a zero divisor in $\mathrm{Mat}_2(K)$, then $(\pi')^{-1}(e)$ consists of elements in $\phi(A_d)$ such that α_i are fixed with $\alpha_1\alpha_4 = \alpha_2\alpha_3$. Now for $f' \in (\pi')^{-1}(e)$, we have $\dim \ker \rho_{f'} = 4$ if and only if the rank of f' is 3. This is if and only if a 3×3 minor of f' is nonzero which is if and only if $\alpha_1\beta_4 + \alpha_4\beta_1 \neq \alpha_2\beta_3 + \alpha_3\beta_2$ by looking at the 3×3 submatrices containing all the β_i. Hence, a generic element in $(\pi')^{-1}(e)$ satisfies $\dim \ker \rho_{f'} = 4$ and so $f = \phi^{-1}(f')$ satisfies $\dim \ker \rho_f = 4$ as required.

□

Let e be a nonzero zero divisor in $A_d/\mathcal{R}(A_d)$, which can be explicitly computed by Corollary 3.4.4 and Remark 3.4.5. We know from the proof of Lemma 3.4.9, whether or not an element in $\pi^{-1}(e)$ gives a dimension 4 left ideal is a homogeneous linear condition. Fix an element $f' \in \pi^{-1}(e)$ and let $\{b_1, b_2, b_3, b_4\}$ be a basis of $\pi^{-1}(e) - f'$. Then at least one of the elements $f', f' + b_i$ $i \in \{1, ..., 4\}$ gives a dimension 4 left ideal as these five points span $\pi^{-1}(e)$ and for a generic element $f \in \pi^{-1}(e)$, $\dim \ker \rho_f = 4$ by Lemma 3.4.9 . So we get the trivialization by further applying Case 1.

3.4.3 Finding nonzero zero divisor over $\mathbb{R}$

In this section, we describe an algorithm that finds a nonzero zero divisor $d \in A$, in the case $K = \mathbb{R}$.

The algorithm starts by picking a random element $c \in A$. We compute its minimal polynomial $m_c(x)$. Suppose $m_c(x)$ is a degree 4 polynomial with no repeated roots. It then factorizes into two quadratic polynomials f_1, f_2 over $\mathbb{R}$ and $f_1(c)$ is a nonzero zero divisor. Note that in this case, the characteristic polynomial of the image of x in $\mathrm{Mat}_4(K)$ under any isomorphism $A \xrightarrow{\phi} \mathrm{Mat}_4(\mathbb{R})$,

denoted by $\chi_c(x)$, is equal to $m_c(x)$ and so also has no repeated roots. We observe that $\chi_c(x)$ has repeated roots if and only if it and its derivative share a common root which is an algebraic condition on the coefficients of $\chi_c(x)$ and hence an algebraic condition on the entries of $\phi(x)$. This implies the set of elements in $\mathrm{Mat}_4(\mathbb{R})$ whose characteristic polynomials have no repeated roots forms a dense Zariski open subset. Hence, we simply pick another random element in A if $m_c(x)$ is not a degree 4 polynomial with no repeated roots.

Remark 3.4.10. Combining the algorithm in Section 3.4.2 in the case $K = \mathbb{R}$ and the algorithm above, we now have an algorithm to trivialize an algebra $A \cong \mathrm{Mat}_4(\mathbb{R})$ that is specified by the structure constants.

3.4.4 Algorithm for trivializing matrix algebra over $\mathbb{Q}$

In this section, we describe an algorithm that solves Problem 3.4.1 in the case $n = 4$. We first give the following definitions and known results. These are also given in [CFO+15, Section 6].

Suppose A is a $\mathbb{Q}$-algebra that is isomorphic to $\mathrm{Mat}_n(\mathbb{Q})$. An *order* in A is a subring $\mathcal{O} \subset A$ whose additive group is a free $\mathbb{Z}$-module of rank n^2. Let $a_1 = 1, a_2, ..., a_{n^2}$ be a $\mathbb{Q}$-basis for A that is also a $\mathbb{Z}$ basis for $\mathcal{O}$. The *discriminant* of $\mathcal{O}$ is defined as

$$\mathrm{Disc}(\mathcal{O}) = \det(\mathrm{Trd}(a_i a_j)),$$

where Trd denotes the reduced trace and $\mathrm{Trd}(a_i a_j) = \mathrm{Tr}(M_i M_j)$ with $a_i \mapsto M_i$ under an isomorphism $A \cong \mathrm{Mat}_n(\mathbb{Q})$. Note this does not depend on the choice of $A \cong \mathrm{Mat}_n(\mathbb{Q})$ by the Noether Skolem theorem. An order $\mathcal{O}$ is *maximal* if it is not a proper subring of any other order in A.

From the definition above, we know an order of A can be viewed as a lattice in $\mathrm{Mat}_{n^2}(\mathbb{R}) \cong \mathbb{R}^{n^2}$. We also have the following known results on lattices. Let $L \subset \mathbb{R}^m$ be a lattice with a choice of basis as the rows of an $m \times m$ matrix B. Then $\det L = |\det B|$ depends only on L and not on B. By the geometry of numbers, we know L contains a nonzero vector x such that

$$||x||^2 \leq c(\det L)^{2/m},$$

where the constant c only depends on m and $||\ ||$ denotes the standard Euclidean norm. The best possible value for c is the Hermite's constant denoted by γ_m. It was shown in [Bli14] that

$$\gamma_m^m \leq (\frac{2}{\pi})^m \Gamma(1 + \frac{m+2}{2})^2.$$

Now suppose $n = 4$ and $A \cong \mathrm{Mat}_4(\mathbb{Q})$. An algorithm that finds such isomorphism explicitly starts by finding a nonzero zero divisor of A. We follow

the same method as in [CFO+15, Section 6] in the case where the algebra is isomorphic to $\mathrm{Mat}_3(\mathbb{Q})$ or $\mathrm{Mat}_5(\mathbb{Q})$. Let $\mathcal{O}$ be a maximal order of A. All maximal orders of A have equal discriminant, denoted by $\mathrm{Disc}(A)$, as shown in [Rei03, Section 25]. We have $\mathrm{Disc}(\mathcal{O}) = \mathrm{Disc}(\mathrm{Mat}_4(\mathbb{Z})) = 1$.

Let $a_1 = 1, a_2, ..., a_{16}$ denote a set of $\mathbb{Q}$-basis for A that is also a $\mathbb{Z}$-basis for $\mathcal{O}$. Let $A_{\mathbb{R}} = A \otimes_{\mathbb{Q}} \mathbb{R}$ and we have $A_{\mathbb{R}} \cong \mathrm{Mat}_4(\mathbb{R})$. By Remark 3.4.10, we can compute such isomorphism explicitly and compute the corresponding basis of $\mathrm{Mat}_4(\mathbb{R})$, denoted by $N_1, ..., N_{16}$. This implies that we can identify $\mathcal{O}$ as a subring of $\mathrm{Mat}_4(\mathbb{R})$ and identify $\mathrm{Mat}_4(\mathbb{R})$ as $\mathbb{R}^{16}$. This makes $\mathcal{O}$ a lattice. Let B be an 16×16 matrix whose rows are basis for $\mathcal{O}$. We have

$$\mathrm{Disc}(\mathcal{O}) = (\det B)^2 \mathrm{Disc}(\mathrm{Mat}_n(\mathbb{Z})).$$

Since $\mathrm{Disc}(\mathcal{O}) = \mathrm{Disc}(\mathrm{Mat}_4(\mathbb{Z})) = 1$, we get $|\det B| = 1$. By the geometry of numbers, $\mathcal{O}$ contains a nonzero element $M \in \mathcal{O} \subset \mathrm{Mat}_4(\mathbb{R})$ such that

$$||M||^2 \leq \gamma_{16},$$

where $\gamma_{16}^{16} \leq (\frac{2}{\pi})^{16} \Gamma(1 + \frac{18}{2})^2$. It can be checked that $\gamma_{16} < 4$. Now by running Gram Schmidt algorithm to columns of M, we can write $M = QR$, where Q is orthogonal and R is upper triangular with diagonal entries $r_1, ..., r_4$. Then by AM-GM inequality:

$$|\det M|^{1/2} = (\prod_{i=1}^{4} r_i^2)^{1/4} \leq \frac{1}{4} \sum_{i=1}^{4} r_i^2 \leq \frac{1}{4} ||R||^2 = \frac{1}{4} ||M||^2 < 1.$$

Since $\mathcal{O}$ is an order, we know $\det M$ is an integer. This implies $\det M = 0$.

Therefore 0 is an eigenvalue of M. This implies that its minimal polynomial $\mu_M(x)$ will have a factor of x and therefore M is a nonzero zero divisor. In practice, we use MAGMA to try some small integer linear combination of the basis $N_1, ..., N_{16}$ and find one that has reducible minimal polynomial.

Now we summarize the algorithm for solving Problem 3.4.1 in the case $n = 4$ that is discussed in this section.

- Compute a maximal order $\mathcal{O} \subset A$ which can be done using MAGMA. See for example [R'o90] [IR93] [Fri] and the MAGMA implementation by de Graaf.
- Trivialize A over $\mathbb{R}$. This is discussed in Remark 3.4.10.
- Embed $\mathcal{O}$ as a lattice in $\mathrm{Mat}_4(\mathbb{R}) \cong \mathbb{R}^{16}$ using the above trivialization.
- Look for small linear combinations of the basis elements of $\mathcal{O}$ that has reducible minimal polynomial which gives a nonzero zero divisor of A.
- Then trivialize A over $\mathbb{Q}$ as discussed in 3.4.2 in the case $K = \mathbb{Q}$.

Remark 3.4.11. In practice, we can compute an LLL-reduced, short and nearly orthogonal, basis for $\mathcal{O}$ after embedding $\mathcal{O} \in \mathbb{R}^{16}$ in the above algorithm. The LLL lattice basis reduction algorithm given in [LLL82] is a polynomial time lattice reduction algorithm that computes an LLL-reduced lattice basis and is implemented in MAGMA. Working with an LLL-reduced basis tends to speed up the MAGMA computation and give a simpler trivialization.

Chapter 4

The Cassels-Tate Pairing with K-Rational Two-Torsion Points

In this chapter, we let J denote the Jacobian variety of a genus two curve $\mathcal{C}$ that is defined by $y^2 = f(x)$ such that f is a degree 6 polynomial defined over the base field K and all roots of f are defined over K. Note that this implies that all points in $J[2]$ are defined over K by Remark 1.2.1. We will prove an explicit formula for the Cassels-Tate pairing on $\text{Sel}^2(J) \times \text{Sel}^2(J)$. In this chapter, the base field K is always a number field, unless stated otherwise. We will then describe an algorithm such that in the case where $K = \mathbb{Q}$, we can compute this explicit formula. This method is a generalization of what was done by Cassels in [Cas98] in the case of elliptic curves. Later on, in [FSS10], the pairing in [Cas98] was proved to be the Cassels-Tate pairing.

4.1 Formula for the Cassels-Tate Pairing

In this section, we state and prove an explicit formula for the Cassels-Tate pairing on $\text{Sel}^2(J) \times \text{Sel}^2(J)$ under the assumption that all points in $J[2]$ are defined over the base field K.

4.1.1 Choice of generators of J[2]

We first explain some notation used in this chapter.

Let the genus two curve $\mathcal{C}$ be of the form

$$\mathcal{C} : y^2 = \lambda(x - \omega_1)(x - \omega_2)(x - \omega_3)(x - \omega_4)(x - \omega_5)(x - \omega_6),$$

where $\lambda, \omega_i \in K$ and $\lambda \neq 0$. Its Jacobian variety is denoted by J.

Define

$$P = \{(\omega_1, 0), (\omega_2, 0)\}, \quad Q = \{(\omega_1, 0), (\omega_3, 0)\},$$
$$R = \{(\omega_4, 0), (\omega_5, 0)\}, \quad S = \{(\omega_4, 0), (\omega_6, 0)\}.$$

We check that they generate $J[2]$ and by Lemma 1.7.6, the Weil pairing among them is represented by W:

$$\begin{bmatrix} 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \end{bmatrix}. \tag{4.1.1}$$

More explicitly, W_{ij} denotes the Weil pairing between the i^{th} and j^{th} generators.

We first recall some discussion in Section 1.10. In Remark 1.10.6, we showed that in the case where f has a root defined over K then $P^1(G_K, J[2]) \cong \{\delta \in L^*/(L^*)^2K^* : N(\delta) \text{ is a square}\}$ where $P^1(G_K, J[2]) = \ker \gamma$ in (1.10.2) and $L = K[x]/(f)$. Since now we assume all roots of f are defined over K, we get that $M = \ker(\mu_2(\bar{L}) \xrightarrow{N} \mu_2(\bar{K}))$ is isomorphic to $\mu_2(\bar{K})^5$ which implies that $H^2(G_K, M) \cong (\mathrm{Br}(K)[2])^5$. Since $\mathrm{Br}(K)[2] \to (\mathrm{Br}(K)[2])^5$ is injective, by the exactness of $H^1(G_K, J[2]) \xrightarrow{\gamma} \mathrm{Br}(K)[2] \to H^2(G_K, M)$, we have γ is the zero map and $P^1(G_K, J[2]) = H^1(G_K, J[2])$. This implies that $H^1(G_K, J[2]) \cong \{\delta \in L^*/(L^*)^2K^* : N(\delta) \text{ is a square}\}$.

We now show that we also have $H^1(G_K, J[2]) \cong (K^*/(K^*)^2)^4$ induced by the generators P, Q, R, S and that the two interpretations of $H^1(G_K, J[2])$ are compatible.

Consider the map $J[2] \xrightarrow{w_2} (\mu_2(\bar{K}))^4$, where w_2 denotes taking the Weil pairing with P, Q, R, S. Since P, Q, R, S form a set of generators of $J[2]$ and the Weil pairing is a nondegerate bilinear pairing, we get that w_2 is injective. This implies that w_2 is an isomorphism as $|J[2]| = |(\mu_2(\bar{K}))^4| = 16$. We then get

$$H^1(G_K, J[2]) \xrightarrow{w_{2,*}} H^1(G_K, (\mu_2(\bar{K}))^4) \cong (K^*/(K^*)^2)^4,$$

where $w_{2,*}$ is induced by w_2 and $\cong$ is the Kummer isomorphism derived from Hilbert's Theorem 90. Since the above map $H^1(G_K, J[2]) \xrightarrow{w_{2,*}} H^1(G_K, (\mu_2(\bar{K}))^4)$ is an isomorphism, we can represent elements in $H^1(G_K, J[2])$ by elements in $(K^*/(K^*)^2)^4$.

Note that we have the following commutative diagram:

$$\begin{array}{ccccccccc} & & J[2] & \xrightarrow[\cong]{w_2} & (\mu_2(\bar{K}))^4 & & & & \\ & & \downarrow{\scriptstyle =} & & \downarrow{\scriptstyle g} & & & & \\ 1 & \longrightarrow & J[2] & \xrightarrow{\alpha} & \frac{\mu_2(\bar{L})}{\mu_2(\bar{K})} & \xrightarrow{N} & \mu_2(\bar{K}) & \longrightarrow & 1, \end{array} \tag{4.1.2}$$

where the bottom exact sequence is given in (1.10.1) and g is an isomorphism $(\mu_2(\bar{K}))^4 \to \ker\left(\mu_2(\bar{L})/\mu_2(\bar{K}) \xrightarrow{N} \mu_2(\bar{K}^*)\right)$ defined by

$$(a, b, c, d) \mapsto (abc, bc, ac, d, cd, 1),$$

with its inverse given by

$$(a_1, a_2, a_3, a_4, a_5, a_6) \mapsto (a_1a_2, a_1a_3, a_4a_5, a_4a_6).$$

Hence, (4.1.2) induces a commutative diagram on the cohomology. Since all roots of f are defined over K, we have $\mu_2(L)/\mu_2(K) \xrightarrow{N} \mu_2(K)$ is surjective which implies that $\alpha_* : H^1(G_K, J[2]) \to H^1(G_K, \mu_2(\bar{L})/\mu_2(\bar{K}))$ induced by α is injective.

$$\begin{array}{ccccccc} & & H^1(G_K, J[2]) & \xrightarrow[\cong]{w_{2,*}} & H^1(G_K, (\mu_2(\bar{K}))^4) & & \\ & & \downarrow{\scriptstyle =} & & \downarrow{\scriptstyle g_*} & & \\ 1 & \longrightarrow & H^1(G_K, J[2]) & \xrightarrow{\alpha_*} & H^1(G_K, \frac{\mu_2(\bar{L})}{\mu_2(\bar{K})}) & \xrightarrow{N_*} & H^1(G_K, \mu_2(\bar{K})), \end{array} \tag{4.1.3}$$

where g_* is the isomorphism induced by g and N_* is induced by N. By a diagram chase, we get $H^1(G_K, (\mu_2(\bar{K}))^4)$ is isomorphic to $\ker\big(H^1(G_K, \mu_2(\bar{L})/\mu_2(\bar{K})) \xrightarrow{N_*} H^1(G_K, \mu_2(\bar{K}))\big)$, which is isomorphic to $\{\delta \in L^*/(L^*)^2K^* : N(\delta) \text{ is a square}\}$. Hence, we have the commutative diagram below that shows the compatibility of the two interpretations of $H^1(G_K, J[2])$.

$$\begin{array}{ccc} H^1(G_K, J[2]) & \xrightarrow[\cong]{w_{2,*}} & H^1(G_K, (\mu_2(\bar{K}))^4) \cong (K^*/(K^*)^2)^4 \\ \downarrow{\scriptstyle =} & & \downarrow{\scriptstyle g_*} \\ H^1(G_K, J[2]) & \xrightarrow[\cong]{\alpha_*} & \{\delta \in \frac{L^*}{(L^*)^2K^*} : N(\delta) \text{ is a square}\}. \end{array}$$

Suppose the image of $\epsilon \in H^1(G_K, J[2])$ in $L^*/(L^*)^2K^*$ via α^* is represented by $\delta \in L^*$ which gives $(a_1, a_2, a_3, a_4, a_5, a_6)$ when evaluating at the 6 roots $\omega_1, ..., \omega_6$. The above commutative diagram implies that under the isomorphism $H^1(G_K, J[2]) \cong (K^*/(K^*)^2)^4$, ϵ corresponds to $(a_1a_2, a_1a_3, a_4a_5, a_4a_6)$.

Remark 4.1.1. Let $S = \{\text{places of bad reduction for } \mathcal{C}\} \cup \{\text{places dividing } 2\} \cup \{\text{infinite places}\}$. Similar to Remark 2.3.3(ii), if we embed $H^1(G_K, J[2]) \xrightarrow{w_{2,*}} (K^*/(K^*)^2)^4$, then the image of any Selmer element is in $K(S, 2)^4$ by Lemma 2.3.2 with $\phi = [2]$.

4.1.2 Statement of the formula

In this section, we give the statement of the theorem on the formula for the Cassels-Tate pairing on $\mathrm{Sel}^2(J) \times \mathrm{Sel}^2(J)$ assuming all points in $J[2]$ are defined over K. Recall that in this thesis, J is principally polarized via the theta divisor Θ, as defined in Section 1.2.3. More specifically, as stated in Section 1.2.4, the polarization $\lambda : J \to J^\vee$ is given by $P \mapsto [\tau_P^*\Theta - \Theta]$. We will first prove the following lemma.

Lemma 4.1.2. *For $\epsilon \in Sel^2(J)$, let $(J_\epsilon, \pi_\epsilon)$ denote the corresponding 2-covering of J. Hence, there exists an isomorphism $\phi_\epsilon : J_\epsilon \to J$ defined over $\bar{K}$ such that $[2] \circ \phi_\epsilon = \pi_\epsilon$. Suppose $T \in J(K)$ and $T_1 \in J(\bar{K})$ satisfy $2T_1 = T$. Then*

(i) There exists a K-rational divisor on J_ϵ, D_T, representing the divisor class of $\phi_\epsilon^*(\tau_{T_1}^*(2\Theta))$.

(ii) Let D, D_T be K-rational divisors on J_ϵ representing the divisor class of $\phi_\epsilon^*(2\Theta)$ and $\phi_\epsilon^*(\tau_{T_1}^*(2\Theta))$ respectively. Then $D_T - D \sim \phi_\epsilon^*(\tau_T^*\Theta - \Theta)$. Suppose T is a two-torsion point. Then $2D_T - 2D$ is a K-rational principal divisor. Hence, there exists a K-rational function f_T on J_ϵ such that $div(f_T) = 2D_T - 2D$.

Proof. By definition of a 2-covering, $[2] \circ \phi_\epsilon = \pi_\epsilon$ is a morphism defined over K. Also, by Proposition 1.5.10, $\phi_\epsilon \circ (\phi_\epsilon^{-1})^\sigma = \tau_{\epsilon_\sigma}$ for all $\sigma \in G_K$, where $(\sigma \mapsto \epsilon_\sigma)$ is a cocycle representing ϵ. Now consider $\tau_{T_1} \circ \phi_\epsilon$, we have $[2] \circ \tau_{T_1} \circ \phi_\epsilon = \tau_T \circ [2] \circ \phi_\epsilon = \tau_T \circ \pi_\epsilon$. Since τ_T is defined over K, $(J_\epsilon, \tau_T \circ \pi_\epsilon)$ is also a 2-covering of J. We get $\tau_{T_1} \circ \phi_\epsilon \circ ((\tau_{T_1} \circ \phi_\epsilon)^{-1})^\sigma = \tau_{T_1} \circ \phi_\epsilon \circ (\phi_\epsilon^{-1})^\sigma \circ \tau_{-\sigma(T_1)} = \tau_{\epsilon_\sigma} \circ \tau_{T_1} \circ \tau_{-\sigma(T_1)}$, for all $\sigma \in G_K$. This implies the 2-covering $(J_\epsilon, \tau_T \circ \pi_\epsilon)$ corresponds to the element in $H^1(G_K, J[2])$ that is represented by the cocycle $(\sigma \mapsto \epsilon_\sigma + T_1 - \sigma(T_1))$. Hence, $(J_\epsilon, \tau_T \circ \pi_\epsilon)$ is the 2-covering of J corresponding to $\epsilon + \delta(T)$, where δ denotes the connecting map that corresponds to $J \xrightarrow{[2]} J$ as in Notation 1.4.1. By Proposition 1.6.2, there exists a Brauer-Severi diagram: $[J_\epsilon \xrightarrow{|\phi_\epsilon^*(\tau_{T_1}^*(2\Theta))|} \mathbb{P}^3]$ and a commutative diagram:

$$\begin{array}{ccc} J_\epsilon & \xrightarrow{|\phi_\epsilon^*(\tau_{T_1}^*(2\Theta))|} & \mathbb{P}^3 \\ \downarrow{\scriptstyle \tau_{T_1} \circ \phi_\epsilon} & & \downarrow{\scriptstyle \psi_\epsilon} \\ J & \xrightarrow{|2\Theta|} & \mathbb{P}^3. \end{array}$$

Recall the morphism $J_\epsilon \xrightarrow{|\phi_\epsilon^*(\tau_{T_1}^*(2\Theta))|} \mathbb{P}^3$ is defined over K. So the pull back of a hyperplane section via this morphism gives us a rational divisor D_T representing the divisor class of $\phi_\epsilon^*(\tau_{T_1}^*(2\Theta))$ as required by (i).

Since the polarization $\lambda : J \to J^\vee$ is an isomorphism and $2T_1 = T$, we have $\phi_\epsilon^*(\lambda(T)) = [\phi_\epsilon^*(\tau_T^*\Theta - \Theta)] = [\phi_\epsilon^*(\tau_{T_1}^*(2\Theta))] - [\phi_\epsilon^*(2\Theta)] = [D_T] - [D]$. The fact

that T is a two-torsion point implies that $2\phi_\epsilon^*(\lambda(P)) = 0$. Hence, $2D_T - 2D$ is a K-rational principal divisor which gives (ii).

□

We now deduce the following remark from Lemma 4.1.2. This is needed in the formula for the Cassels-Tate pairing on $\mathrm{Sel}^2(J) \times \mathrm{Sel}^2(J)$.

Remark 4.1.3. We now apply Lemma 4.1.2(i) to $T = \mathcal{O}_J, P, Q, R, S \in J[2]$ and obtain $D = D_{\mathcal{O}_J}, D_P, D_Q, D_R, D_S$. Then we apply Lemma 4.1.2(ii) to D and D_T for $D_T = D_P, D_Q, D_R, D_S$. Therefore, D denotes a K-rational divisor on J_ϵ representing the divisor class of $\phi_\epsilon^*(2\Theta)$ and D_P denotes a K-rational divisor on J_ϵ representing the divisor class of $\phi_\epsilon^*(\tau_{P_1}^*(2\Theta))$, for some P_1 such that $2P_1 = P$. Moreover, $D_P - D \sim \phi_\epsilon^*(\tau_P^*\Theta - \Theta)$. We have similar statements that hold for D_Q, D_R, D_S. Furthermore, there exist K-rational functions f_P, f_Q, f_R, f_S on J_ϵ such that $\mathrm{div}(f_T) = 2D_T - 2D$ for $T = P, Q, R, S$.

Theorem 4.1.4. *Let J be the Jacobian variety of a genus two curve $\mathcal{C}$ defined over a number field K where all points in $J[2]$ are defined over K. For any $\epsilon, \eta \in Sel^2(J)$, let $(J_\epsilon, [2] \circ \phi_\epsilon)$ be the 2-covering of J corresponding to ϵ where $\phi_\epsilon : J_\epsilon \to J$ is an isomorphism defined over $\bar{K}$. Fix a choice of $\{P, Q, R, S\}$, generators of $J[2]$, that satisfy the Weil pairing matrix (4.1.1). Let (a, b, c, d) denote the image of η via $H^1(G_K, J[2]) \cong (K^*/(K^*)^2)^4$, which is induced by taking Weil pairing with $\{P, Q, R, S\}$ as explained in Section 4.1.1. Then there exist f_P, f_Q, f_R, f_S, K-rational functions on J_ϵ, such that*

$$\langle \epsilon, \eta \rangle_{CT} = \prod_{\text{place } v} (f_P(P_v), b)_v (f_Q(P_v), a)_v (f_R(P_v), d)_v (f_S(P_v), c)_v,$$

where $(\ ,\ )_v$ denotes the Hilbert symbol for a given place v of K and P_v is an arbitrary choice of a local point on J_ϵ avoiding the zeros and poles of these f_P, f_Q, f_R, f_S.

Remark 4.1.5. In Section 4.4, we will show that the formula for the Cassels-Tate pairing on $\mathrm{Sel}^2(J) \times \mathrm{Sel}^2(J)$ given in Theorem 4.1.4 is in fact always a finite product.

4.1.3 Proof of the formula

In this section, we give a proof for Theorem 4.1.4. We need to first quote the following lemma which can be proved via explicitly computing the difference of the two cocycles as a coboundary element.

Lemma 4.1.6. [Ser79, Chapter XIV, Section 2, Proposition 5] *Let $a, b \in \bar{K}^*$ for some perfect field K. The following two cocycles represent the same element*

in $H^2(G_K, \bar{K}^*)$*:*

(i)

$$(\sigma, \tau) \mapsto \begin{cases} b & \text{if } \sigma(\sqrt{a})/\sqrt{a} = \tau(\sqrt{a})/\sqrt{a} = -1, \\ 1 & \text{otherwise} \end{cases}$$

(ii)

$$(\sigma, \tau) \mapsto \begin{cases} -1 & \text{if } \sigma(\sqrt{a})/\sqrt{a} = \tau(\sqrt{b})/\sqrt{b} = -1, \\ 1 & \text{otherwise} \end{cases}$$

Furthermore, by Remark 1.4.16, we know they both represent the equivalence class of the quaternion algebra (a, b) *in* $Br(K) \cong H^2(G_K, \bar{K}^*)$.

Now we prove Theorem 4.1.4.

Proof of Thoerem 4.1.4. We will show that the formula given in the theorem is the same as the homogeneous space definition of the Cassels-Tate pairing defined in Section 1.8.2.

We know $\eta \in H^1(G_K, J[2])$ corresponds to $(a, b, c, d) \in (K^*/(K^*)^2)^4$ via taking the Weil pairing with P, Q, R, S, as explained in Section 4.1.1. Hence, η is represented by the following cocycle

$$(\sigma \mapsto \tilde{b}_\sigma P + \tilde{a}_\sigma Q + \tilde{d}_\sigma R + \tilde{c}_\sigma S),$$

where $\sigma \in G_K$ and for each element $x \in K^*/(K^*)^2$, we define $\tilde{x}_\sigma \in \{0, 1\}$ such that $(-1)^{\tilde{x}_\sigma} = \sigma(\sqrt{x})/\sqrt{x}$.

Then the corresponding image of η in $H^1(G_K, \mathrm{Pic}^0(J_\epsilon))$ is represented by the cocycle that sends $\sigma \in G_K$ to

$$\tilde{b}_\sigma \phi_\epsilon^*[\tau_P^*\Theta - \Theta] + \tilde{a}_\sigma \phi_\epsilon^*[\tau_Q^*\Theta - \Theta] + \tilde{d}_\sigma \phi_\epsilon^*[\tau_R^*\Theta - \Theta] + \tilde{c}_\sigma \phi_\epsilon^*[\tau_S^*\Theta - \Theta].$$

By Remark 4.1.3, there exist K-rational divisors D_P, D_Q, D_R, D_S on J_ϵ such that the above cocycle sends $\sigma \in G_K$ to

$$\tilde{b}_\sigma[D_P - D] + \tilde{a}_\sigma[D_Q - D] + \tilde{d}_\sigma[D_R - D] + \tilde{c}_\sigma[D_S - D].$$

Now we need to map this element in $H^1(G_K, \mathrm{Pic}^0(J_\epsilon))$ to an element in $H^2(G_K, \bar{K}(J_\epsilon)^*/\bar{K}^*)$ via the connecting map induced by the short exact sequence $0 \to \bar{K}(J_\epsilon)^*/\bar{K}^* \to \mathrm{Div}^0(J_\epsilon) \to \mathrm{Pic}^0(J_\epsilon) \to 0$. Hence, by the formula for the connecting map as in Section 1.4 and the fact that the divisors D, D_P, D_Q, D_R, D_S are all K-rational, we get that the corresponding element in $H^2(G_K, \bar{K}(J_\epsilon)^*/\bar{K}^*)$ has image in $H^2(G_K, \mathrm{Div}^0(J_\epsilon))$ represented by the following cocycle:

$$(\sigma,\tau) \mapsto (\tilde{b}_\tau - \tilde{b}_{\sigma\tau} + \tilde{b}_\sigma)(D_P - D) + (\tilde{a}_\tau - \tilde{a}_{\sigma\tau} + \tilde{a}_\sigma)(D_Q - D) + (\tilde{d}_\tau - \tilde{d}_{\sigma\tau} + \tilde{d}_\sigma)(D_R - D) + (\tilde{c}_\tau - \tilde{c}_{\sigma\tau} + \tilde{c}_\sigma)(D_S - D), \text{ for } \sigma,\tau \in G_K.$$

It can be checked that, for $x \in K^*/(K^*)^2$ and $\sigma,\tau \in G_K$, we get $\tilde{x}_\tau - \tilde{x}_{\sigma\tau} + \tilde{x}_\sigma = 2$ if both σ and τ flip $\sqrt{x}$ and otherwise it is equal to zero. Define $\iota_{\sigma,\tau,x} = 1$ if both σ and τ flip $\sqrt{x}$ and otherwise $\iota_{\sigma,\tau,x} = 0$. Note that the map that sends $x \in K^*/(K^*)^2$ to the class of $((\sigma,\tau) \mapsto \iota_{\sigma,\tau,x})$ explicitly realizes the map $K^*/(K^*)^2 \cong H^1(G_K, 1/2\mathbb{Z}/\mathbb{Z}) \subset H^1(G_K, \mathbb{Q}/\mathbb{Z}) \to H^2(G_K, \mathbb{Z})$. Then, for $\sigma,\tau \in G_K$, the cocycle in the last paragraph sends (σ,τ) to

$$\iota_{\sigma,\tau,b} \cdot 2(D_P - D) + \iota_{\sigma,\tau,a} \cdot 2(D_Q - D) + \iota_{\sigma,\tau,d} \cdot 2(D_R - D) + \iota_{\sigma,\tau,c} \cdot 2(D_S - D).$$

Hence, by Remark 4.1.3, there exist K-rational functions f_P, f_Q, f_R, f_S on J_ϵ such that the corresponding element in $H^2(G_K, \bar{K}(J_\epsilon)^*/\bar{K}^*)$ is represented by

$$(\sigma,\tau) \mapsto [f_P^{\iota_{\sigma,\tau,b}} \cdot f_Q^{\iota_{\sigma,\tau,a}} \cdot f_R^{\iota_{\sigma,\tau,d}} \cdot f_S^{\iota_{\sigma,\tau,c}}], \text{ for all } \sigma,\tau \in G_K.$$

For each place v of K, following the homogeneous space definition of $\langle \epsilon, \eta \rangle_{CT}$, we obtain an element in $H^2(G_{K_v}, \bar{K}_v^*)$ from the long exact sequence induced by the short exact sequence $0 \to \bar{K}_v^* \to \bar{K}_v(J_\epsilon)^* \to \bar{K}_v(J_\epsilon)^*/\bar{K}_v^* \to 0$. This element in $H^2(G_{K_v}, \bar{K}_v^*)$ can be represented by

$$(\sigma,\tau) \mapsto f_P(P_v)^{\iota_{\sigma,\tau,b}} \cdot f_Q(P_v)^{\iota_{\sigma,\tau,a}} \cdot f_R(P_v)^{\iota_{\sigma,\tau,d}} \cdot f_S(P_v)^{\iota_{\sigma,\tau,c}}, \text{ for all } \sigma,\tau \in G_K,$$

for some local point $P_v \in J_\epsilon(K_v)$ avoiding the zeros and poles of f_P, f_Q, f_R, f_S by Remark 1.8.7(i).

Hence, by Lemma 4.1.6, the above element in $\mathrm{Br}(K_v) \cong H^2(G_{K_v}, \bar{K}_v^*)$ is the class of the tensor product of quaternion algebras

$$(f_P(P_v), b) + (f_Q(P_v), a) + (f_R(P_v), d) + (f_S(P_v), c).$$

Then, by Lemma 1.4.19,

$$\begin{aligned}&\mathrm{inv}\big((f_P(P_v), b) + (f_Q(P_v), a) + (f_R(P_v), d) + (f_S(P_v), c)\big)\\ &= (f_P(P_v), b)_v (f_Q(P_v), a)_v (f_R(P_v), d)_v (f_S(P_v), c)_v,\end{aligned}$$

where $(\ ,\ )_v$ denotes the Hilbert symbol: $K_v^* \times K_v^* \to \{1, -1\}$, as required.

□

4.2 Explicit Computation

In this section, we explain how we explicitly compute the Cassels-Tate pairing on $\mathrm{Sel}^2(J) \times \mathrm{Sel}^2(J)$ using the formula given in Theorem 4.1.4, under the assumption that all points in $J[2]$ are defined over K. We fix $\epsilon \in \mathrm{Sel}^2(J)$ and $(J_\epsilon, [2]\circ\phi_\epsilon)$, the 2-covering of J corresponding to ϵ with $\phi_\epsilon : J_\epsilon \subset \mathbb{P}^{15} \to J \subset \mathbb{P}^{15}$ given in Theorem 1.11.1. The statement of Theorem 4.1.4 suggests that we need to compute the K-rational divisors D, D_P, D_Q, D_R, D_S on J_ϵ and the K-rational function f_P, f_Q, f_R, f_S on J_ϵ, as in Remark 4.1.3.

4.2.1 Modified naive method

Recall that in Sections 3.2 and 3.3, we described two general methods for computing a linear isomorphism $\psi_\epsilon : \mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ corresponding to ϵ. More explicitly, we have $\psi_\epsilon(\psi_\epsilon^{-1})^\sigma$ is the action of translation by $\epsilon_\sigma \in J[2]$ on $\mathcal{K}$ and $(\sigma \mapsto \epsilon_\sigma)$ is a cocycle representing ϵ, as explained in the beginning of Section 3.2. Since all points in $J[2]$ are defined over K, we can in fact simplify the naive method.

By Lemma 3.2.1, we have an explicit formula for M_T that represents the action of translation by $T \in J[2]$ on the Kummer surface $\mathcal{K} \subset \mathbb{P}^3$ and $\{M_T, T \in J[2]\}$ form a basis of $\mathrm{Mat}_4(\bar{K})$. Since all points in $J[2]$ are defined over K, we get $M_T \in \mathrm{Mat}_4(K)$, and $\{M_T, T \in J[2]\}$ forms a basis of $\mathrm{Mat}_4(K)$. We follow the notation of the étale algebra R as in the Section 3.1.3. Define $\xi \in (R \otimes R)^*$ such that $M_{T_1} M_{T_2} = \xi(T_1, T_2) M_{T_1+T_2}$ and $c_P, c_Q, c_R, c_S \in K$ such that

$$M_P^2 = c_P I, M_Q^2 = c_Q I, M_R^2 = c_R I, \text{ and } M_S^2 = c_S I.$$

The explicit formulae for c_P, c_Q, c_R, c_S can also be found in [CF96, Chapter 3 Section 2]. Moreover, by [CF96, Chapter 3 Section 3] and the Weil pairing relationship among the generators P, Q, R, S of $J[2]$ specified by (4.1.1), we know that $[M_P, M_Q] = [M_R, M_S] = -I$ and the commutators of the other pairs are trivial.

By the discussion at the end of Section 3.2.2, to compute a linear isomorphism $\psi_\epsilon : \mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ corresponding to ϵ, it suffices to first compute a set of basis $\{M'_T, T \in J[2]\}$ for $\mathrm{Mat}_4(K)$ such that $M'_{T_1} M'_{T_2} = \xi_\epsilon(T_1, T_2) M'_{T_1+T_2}$, where $\xi_\epsilon = \xi\rho$ with ρ given in Remark 3.2.4. Then one such ψ_ϵ is represented by $B \in \mathrm{Mat}_4(\bar{K})$ with $M'_T = B^{-1} M_T B \in \mathrm{PGL}_4(\bar{K})$ for all $T \in J[2]$. Recall that $T \mapsto M'_T$ is a Galois equivariant section for $\mathbf{\Theta}_\epsilon \to J[2]$. As explained in Remark 3.2.9, in fact we only need to compute M'_P, M'_Q, M'_R, M'_S. We observe that M'_P, M'_Q, M'_R, M'_S generate $\mathrm{Mat}_4(K)$ as P, Q, R, S generate $J[2]$ and $M'_{T_1} M'_{T_2}$ is a multiple of $M'_{T_1+T_2}$ for any $T_1, T_2 \in J[2]$ by construction. Hence, in the section, we discuss how to find such matrices explicitly without the algorithm in Section 3.4 which is needed in the general case.

Suppose $(a_\epsilon, b_\epsilon, c_\epsilon, d_\epsilon) \in (K^*/(K^*)^2)^4$ represents ϵ as in Section 4.1.1. By the formula for ρ in Remark 3.2.4, we know that $M_P'^2 = c_P a_\epsilon I, M_Q'^2 = c_Q b_\epsilon I, M_R'^2 = c_R c_\epsilon I, M_S'^2 = c_S d_\epsilon I$. Also, by Definition 3.1.2, we have $[M_P', M_Q'] = [M_R', M_S'] = -I$ and the commutators of the other pairs are trivial. This implies that

$$\mathrm{Mat}_4(K) \cong (c_P a_\epsilon, c_Q b_\epsilon) \otimes (c_R c_\epsilon, c_S d_\epsilon)$$
$$M_P' \mapsto i_1 \otimes 1, M_Q' \mapsto j_1 \otimes 1, M_R' \mapsto 1 \otimes i_2, M_S' \mapsto 1 \otimes j_2,$$

where the generators of $(c_P a_\epsilon, c_Q b_\epsilon)$ are i_1, j_1 and the generators of $(c_R c_\epsilon, c_S d_\epsilon)$ are i_2, j_2.

Let $A = (c_P a_\epsilon, c_Q b_\epsilon), B = (c_R c_\epsilon, c_S d_\epsilon)$. By the argument above, we know $A \otimes B$ represents the trivial element in $\mathrm{Br}(K)$ and an explicit isomorphism $A \otimes B \cong \mathrm{Mat}_4(K)$ gives us the explicit matrices M_P', M_Q', M_R', M_S' required. Since the classes of A, B are in $\mathrm{Br}[2]$, we have A, B representing the same element in $\mathrm{Br}(K)$. This implies that $A \cong B$ over K, by Remark 1.4.10. We have the following lemma.

Lemma 4.2.1. *Given a tensor product of two quaternion algebras $A \otimes B$, where $A = (\alpha, \beta)$ $B = (\gamma, \delta)$, with generators i_1, j_1 and i_2, j_2 respectively. Suppose there is an isomorphism $\psi : B \xrightarrow{\sim} A$ given by*

$$i_2 \mapsto a_1 \cdot 1 + b_1 \cdot i_1 + c_1 \cdot j_1 + d_1 \cdot i_1 j_1$$

$$j_2 \mapsto a_2 \cdot 1 + b_2 \cdot i_1 + c_2 \cdot j_1 + d_2 \cdot i_1 j_1,$$

then we have explicit formula for

$$A \otimes B \cong Mat_4(K)$$

where

$$i_1 \otimes 1 \mapsto M_{i_1} := \begin{bmatrix} 0 & \alpha & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$j_1 \otimes 1 \mapsto M_{j_1} := \begin{bmatrix} 0 & 0 & \beta & 0 \\ 0 & 0 & 0 & -\beta \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}$$

$$1 \otimes i_2 \mapsto M_{i_2} := \begin{bmatrix} a_1 & b_1 \cdot \alpha & c_1 \cdot \beta & -d_1 \cdot \alpha\beta \\ b_1 & a_1 & -d_1 \cdot \beta & c_1 \cdot \beta \\ c_1 & d_1 \cdot \alpha & a_1 & -b_1 \cdot \alpha \\ d_1 & c_1 & -b_1 & a_1 \end{bmatrix}$$

$$1 \otimes j_2 \mapsto M_{j_2} := \begin{bmatrix} a_2 & b_2 \cdot \alpha & c_2 \cdot \beta & -d_2 \cdot \alpha\beta \\ b_2 & a_2 & -d_2 \cdot \beta & c_2 \cdot \beta \\ c_2 & d_2 \cdot \alpha & a_2 & -b_2 \cdot \alpha \\ d_2 & c_2 & -b_2 & a_2 \end{bmatrix}$$

Proof. Recall Remark 1.4.5 says that $A \otimes A^{op}$ is isomorphic to a matrix algebra. More specifically, $A \otimes A^{op} \cong \mathrm{End}_K(A)$ via $u \otimes v \mapsto (x \mapsto uxv)$, which makes $A \otimes A^{op} \cong \mathrm{Mat}_4(K)$ after picking a basis for A. Hence,

$$\begin{array}{ccc} A \otimes B^{op} & \cong & \mathrm{Mat}_4(K) \\ u \otimes v & \mapsto & (x \mapsto ux\psi(v)). \end{array}$$

More explicitly, fixing the basis of A to be $\{1, i_1, j_1, i_1 j_1\}$, the isomorphism is given as in the lemma.

□

Hence, by taking $A = (c_P a_\epsilon, c_Q b_\epsilon), B = (c_R c_\epsilon, c_S d_\epsilon)$ in Lemma 4.2.1 above, we can compute the M'_P, M'_Q, M'_S, M'_R provided we can explicitly find an isomorphism $\psi : B \cong A$. We now give an explicit and practical algorithm for finding an isomorphism between two quaternion algebras over $\mathbb{Q}$ that are known to be isomorphic. First we have the following lemma.

Lemma 4.2.2. *Let A be the quaternion algebra (a, b) over $\mathbb{Q}$, where $a, b \in \mathbb{Q}^*$. Let $w \neq 0, 1$ be a squarefree integer. The following are equivalent.*

(i) The algebra A contains a subalgebra isomorphic to $\mathbb{Q}(\sqrt{w})$.

(ii) There exist $s, t, u \in \mathbb{Q}$ with $as^2 + bt^2 - abu^2 = w$.

Proof. Explicitly, A has $\mathbb{Q}$-basis $1, i, j, ij$ and multiplication determined by $i^2 = a$, $j^2 = b$ and $ij = -ji$. Suppose $x \in A$ is given as $r + si + tj + uij$ where $r, s, t, u \in \mathbb{Q}$. We compute

$$x^2 = r^2 + as^2 + bt^2 - abu^2 + 2r(si + tj + uij).$$

Then $x^2 = w$ if and only if $r = 0$ and the equation in (ii) is satisfied.

□

Corollary 4.2.3. *Let $A = (a, b)$ and $B = (c, d)$ be two isomorphic quaternion algebras over $\mathbb{Q}$. There is an explicit and practical algorithm for finding such an isomorphism $A \cong B$.*

Proof. Let i_1, j_1 denote the generators of A. We can assume a, b, c, d are squarefree integers after multiplying by suitable squares. If $c = d = 1$, then we are done by Corollary 3.4.4. Otherwise, we can assume $c \neq 1$. Since $A \cong B$, we know A has a subalgebra $\mathbb{Q}(\sqrt{c})$. By Lemma 4.2.2, there exist $s_1, t_1, u_1 \in \mathbb{Q}$ such that $as_1^2 + bt_1^2 - abu_1^2 = c$. Let $\alpha = s_1 i_1 + t_1 j_1 + u_1 i_1 j_1 \in A$. Now we look for $s_2, t_2, u_2 \in \mathbb{Q}$ that satisfies

$$\alpha(s_2 i_1 + t_2 j_1 + u_2 i_1 j_1) = -(s_2 i_1 + t_2 j_1 + u_2 i_1 j_1)\alpha.$$

Let $\beta = s_2 i_1 + t_2 j_1 + u_2 i_1 j_1 \in A$. Define $e = as_2^2 + bt_2^2 - abu_2^2$ and we have $\beta^2 = e$. Consider the quaternion algebra (c, e) with generators denoted by i_2, j_2. We have an explicit isomorphism $(c, e) \cong A$ such that

$$i_2 \mapsto \alpha, j_2 \mapsto \beta.$$

Then, by Lemma 3.4.2, we compute an explicit isomorphism $(c, d) \cong (c, e)$. The composition of these two isomorphisms give $B \cong A$, as required.

□

4.2.2 Explicit computation of D

In this section, we explain a method for computing the K-rational divisor D on J_ϵ representing the divisor class $\phi_\epsilon^*(2\Theta)$. The idea is to compute it via the commutative diagram of Brauer-Severi diagrams (1.6.2) as in Remark 1.6.3.

Recall, by Theorem 1.11.1, we have an explicit isomorphism $J_\epsilon \subset \mathbb{P}^{15} \xrightarrow{\phi_\epsilon} J \subset \mathbb{P}^{15}$ and we let $u_0, ..., u_9, v_1, ..., v_6$ denote the coordinates of the ambient space of $J_\epsilon \subset \mathbb{P}^{15}$, $k_{11}, k_{12}, ..., k_{44}, b_1, ..., b_6$ denote the coordinates of the ambient space of $J \subset \mathbb{P}^{15}$. Moreover, ϕ_ϵ is represented by a block diagonal matrix consisting of a block of size 10 corresponding to the even basis elements and a block of size 6 corresponding to the odd basis elements. Via Section 4.2.1, we have an explicit isomorphism $\psi_\epsilon : \mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ corresponding to ϵ and we let $k'_1, ..., k'_4$ denote the coordinates of the ambient space of $\mathcal{K}_\epsilon \subset \mathbb{P}^3$. Suppose $\phi_\epsilon(\phi_\epsilon^{-1})^\sigma$ and $\psi_\epsilon(\psi_\epsilon^{-1})^\sigma$ both give the action of translation by some $\epsilon_\sigma \in J[2]$ such that $(\sigma \mapsto \epsilon_\sigma)$ represents $\epsilon \in \mathrm{Sel}^2(J)$. Observe that since all points in $J[2]$ are defined over K, this condition is automatic.

Define $k'_{ij} = k'_i k'_j$. The isomorphism $\psi_\epsilon : \mathcal{K}_\epsilon \subset \mathbb{P}^3_{k'_i} \to \mathcal{K} \subset \mathbb{P}^3_{k_i}$, induces a natural isomorphism $\tilde{\psi}_\epsilon : \mathbb{P}^9_{k'_{ij}} \to \mathbb{P}^9_{k_{ij}}$. More explicitly, suppose ψ_ϵ is represented by the 4×4 matrix A where $(k'_1 : ... , k'_4) \mapsto (\sum_{i=1}^4 A_{1i}k'_i : ... : \sum_{i=1}^4 A_{4i}k'_i)$. Then $\tilde{\psi}_\epsilon : \mathbb{P}^9_{k'_{ij}} \to \mathbb{P}^9_{k_{ij}}$ is given by $(k'_{11} : k'_{12} : ... : k'_{44}) \mapsto (\sum_{i,j=1}^4 A_{1i}A_{1j}k'_{ij} : \sum_{i,j=1}^4 A_{1i}A_{2j}k'_{ij} : ... : \sum_{i,j=1}^4 A_{4i}A_{4j}k'_{ij})$. We have the following commutative diagram which also give embeddings of $\mathcal{K}, \mathcal{K}_\epsilon$ in $\mathbb{P}^9$.

$$\begin{array}{ccc} \mathcal{K}_\epsilon \subset \mathbb{P}^9_{k'_{ij}} & \xrightarrow{g_2} & \mathcal{K}_\epsilon \subset \mathbb{P}^3_{k'_i} \\ \downarrow{\scriptstyle \tilde{\psi}_\epsilon} & & \downarrow{\scriptstyle \psi_\epsilon} \\ \mathcal{K} \subset \mathbb{P}^9_{k_{ij}} & \xrightarrow{g_1} & \mathcal{K} \subset \mathbb{P}^3_{k_i}, \end{array}$$

where $g_1 : (k_{11} : ... : k_{44}) \mapsto (k_{11} : ... : k_{14})$ and $g_2 : (k'_{11} : ... : k'_{44}) \mapsto (k'_{11} : ... : k'_{14})$ are the projection maps. We observe the natural morphisms $(k_1 : ... : k_4) \mapsto (k_{11} : k_{12} : ... : k_{44})$ and $(k'_1 : ... : k'_4) \mapsto (k'_{11} : k'_{12} : ... : k'_{44})$ are the inverses of g_1 and g_2, when restricted to $\mathcal{K}$ and $\mathcal{K}_\epsilon$ respectively. We also note that $\mathcal{K}_\epsilon$ and $\mathcal{K}$ do not lie on any hyperplane in $\mathbb{P}^9$. This makes

$\tilde{\psi}_\epsilon : \mathbb{P}^9_{k'_{ij}} \to \mathbb{P}^9_{k_{ij}}$ the natural map, as it is the unique extension of the morphism $\mathcal{K}_\epsilon \subset \mathbb{P}^9_{k'_{ij}} \to \mathcal{K} \subset \mathbb{P}^9_{k_{ij}}$ that makes the above diagram commute.

On the other hand, the isomorphism $\phi_\epsilon : J_\epsilon \subset \mathbb{P}^{15}_{\{u_i,v_i\}} \to J \subset \mathbb{P}^{15}_{\{k_{ij},b_i\}}$ induces a natural isomorphism $\tilde{\phi}_\epsilon : \mathbb{P}^9_{u_i} \to \mathbb{P}^9_{k_{ij}}$ represented by the 10×10 block of the matrix representing ϕ_ϵ. Since $\phi_\epsilon(\phi_\epsilon^{-1})^\sigma$ and $\psi_\epsilon(\psi_\epsilon^{-1})^\sigma$ both give the action of translation by some $\epsilon_\sigma \in J[2]$, we get $\tilde{\phi}_\epsilon(\tilde{\phi}_\epsilon{}^{-1})^\sigma = \tilde{\psi}_\epsilon(\tilde{\phi}_\epsilon{}^{-1})^\sigma$. Therefore, we get $\tilde{\psi}_\epsilon{}^{-1}\tilde{\phi}_\epsilon$ defined over K and the following commutative diagram that decomposes the standard commutative diagram (1.6.2):

$$\begin{array}{ccccccc}
J_\epsilon \subset \mathbb{P}^{15}_{\{u_i,v_i\}} & \xrightarrow{proj} & \mathbb{P}^9_{u_i} & \xrightarrow{(\tilde{\psi}_\epsilon)^{-1}\tilde{\phi}_\epsilon} & \mathbb{P}^9_{k'_{ij}} & \xrightarrow{g_2} & \mathcal{K}_\epsilon \subset \mathbb{P}^3_{k'_i} \\
\downarrow{\scriptstyle \phi_\epsilon} & & & \searrow^{\tilde{\phi}_\epsilon} \quad \swarrow_{\tilde{\psi}_\epsilon} & & & \downarrow{\scriptstyle \psi_\epsilon} \\
J \subset \mathbb{P}^{15}_{\{k_{ij},b_i\}} & \xrightarrow{proj} & & \mathbb{P}^9_{k_{ij}} & \xrightarrow{g_1} & & \mathcal{K} \subset \mathbb{P}^3_{k_i},
\end{array} \tag{4.2.1}$$

The composition of the morphisms on the bottom gives the standard morphism $J \xrightarrow{|2\Theta|} \mathcal{K} \subset \mathbb{P}^3$ and the composition of the morphisms on the top gives $J_\epsilon \xrightarrow{|\phi_\epsilon^*(2\Theta)|} \mathcal{K}_\epsilon \subset \mathbb{P}^3$.

Let D be the pull back on J_ϵ via $J_\epsilon \subset \mathbb{P}^{15}_{\{u_i,v_i\}} \xrightarrow{proj} \mathbb{P}^9_{u_i} \xrightarrow{(\tilde{\psi}_\epsilon)^{-1}\tilde{\phi}_\epsilon} \mathbb{P}^9_{k'_{ij}} \xrightarrow{proj} \mathbb{P}^3_{k'_i}$ of the hyperplane section given by $k'_1 = 0$. This implies that D is a K-rational divisor on J_ϵ representing the class of $\phi_\epsilon^*(2\Theta)$. Moreover, the pull back on J_ϵ via $J_\epsilon \subset \mathbb{P}^{15}_{\{u_i,v_i\}} \xrightarrow{proj} \mathbb{P}^9_{u_i} \xrightarrow{(\tilde{\psi}_\epsilon)^{-1}\tilde{\phi}_\epsilon} \mathbb{P}^9_{k'_{ij}}$ of the hyperplane section given by $k'_{11} = 0$ is $2D$.

4.2.3 Explicit computation of D_P, D_Q, D_R, D_S

In this section, we explain how to explicitly compute the K-rational divisors D_P, D_Q, D_R, D_S defined in Remark 4.1.3. More explicitly, for $T \in J[2]$, we give a method for computing a K-rational divisor D_T on J_ϵ representing the divisor class of $\phi_\epsilon^*(\tau_{T_1}^*(2\Theta))$ for some T_1 on J such that $2T_1 = T$. Recall that we assume all points in $J[2]$ are defined over K and we have an explicit isomorphism $\phi_\epsilon : J_\epsilon \to J$ such that $(J_\epsilon, [2] \circ \phi_\epsilon)$ is the 2-covering of J corresponding to $\epsilon \in \mathrm{Sel}^2(J)$. Let δ denote the connecting map $J(K)/2J(K) \to H^1(G_K, J[2])$ induced by the short exact sequence given by $J \xrightarrow{2} J$ as in Notation 1.4.1. We let $\delta(T)$ denote the image of the equivalence class of T and first prove the following lemma.

Lemma 4.2.4. *Let $T \in J(K)$. Suppose $\phi_{\epsilon+\delta(T)} : J_{\epsilon+\delta(T)} \to J$ is an isomorphism and $(J_{\epsilon+\delta(T)}, [2] \circ \phi_{\epsilon+\delta(T)})$ is the 2-covering of J corresponding to $\epsilon + \delta(T) \in H^1(G_K, J[2])$. Let $T_1 \in J$ such that $2T_1 = T$. Then, $\phi^{-1}_{\epsilon+\delta(T)} \circ \tau_{T_1} \circ \phi_\epsilon : J_\epsilon \to J_{\epsilon+\delta(T)}$ is defined over K.*

Proof. Using the same argument as in the proof of Lemma 4.1.2(i), we know that $(J_\epsilon, [2]\circ\tau_{T_1}\circ\phi_\epsilon)$ is the 2-covering of J corresponding to $\epsilon+\delta(T) \in H^1(G_K, J[2])$. Since all points in $J[2]$ are defined over K, we have $\tau_{T_1}\circ\phi_\epsilon\circ((\tau_{T_1}\circ\phi_\epsilon)^{-1})^\sigma = \phi_{\epsilon+\delta(T)}\circ(\phi^{-1}_{\epsilon+\delta(T)})^\sigma$, as required.

□

Let $T \in J(K)$ with $2T_1 = T$. Consider the commutative diagram below, the composition of the morphisms in red is defined over K by Lemma 4.2.4. Then the pull back on J_ϵ via the red arrows of a hyperplane section on $\mathcal{K}_{\epsilon+\delta(T)} \subset \mathbb{P}^3$ is a K-rational divisor D_T on J_ϵ representing the divisor class $\phi^*_\epsilon(\tau^*_{T_1}(2\Theta))$. We note that in the case where $T \in J[2]$, the composition of the vertical maps on the left hand side of the the diagram below is in fact given by a 16×16 matrix defined over K even though the individual maps are not defined over K.

$$\begin{array}{ccc}
J_\epsilon \subset \mathbb{P}^{15} & \xrightarrow{|\phi^*_\epsilon(2\Theta)|} & \mathcal{K}_\epsilon \subset \mathbb{P}^3 \\
\downarrow{\scriptstyle \phi_\epsilon} & & \downarrow{\scriptstyle \psi_\epsilon} \\
J \subset \mathbb{P}^{15} & \xrightarrow{|2\Theta|} & \mathcal{K} \subset \mathbb{P}^3 \\
\downarrow{\scriptstyle \tau_{T_1}} & & \\
J \subset \mathbb{P}^{15} & \xrightarrow{|2\Theta|} & \mathcal{K} \subset \mathbb{P}^3 \\
\downarrow{\scriptstyle \phi^{-1}_{\epsilon+\delta(T)}} & & \uparrow{\scriptstyle \psi_{\epsilon+\delta(T)}} \\
J_{\epsilon+\delta(T)} \subset \mathbb{P}^{15} & \xrightarrow{|\phi^*_{\epsilon+\delta(T)}(2\Theta)|} & \mathcal{K}_{\epsilon+\delta(T)} \subset \mathbb{P}^3.
\end{array}$$

Notice that the bottom horizontal morphism $J_{\epsilon+\delta(T)} \xrightarrow{|\phi^*_{\epsilon+\delta(T)}(2\Theta)|} \mathcal{K}_{\epsilon+\delta(T)} \subset \mathbb{P}^3$ can be explicitly computed using the algorithm corresponding to the Selmer element $\epsilon+\delta(T)$ described in Section 4.2.2. Also, by Theorem 1.11.1, we have explicit formulae for ϕ_ϵ and $\phi_{\epsilon+\delta(T)}$. Hence, to explicitly compute D_T, we need to find a way to deal with τ_{T_1}, for some T_1 such that $2T_1 = T$.

Since we need to apply the above argument to $T = P, Q, R, S$, the generators for $J[2]$, we need to deal with the explicit computation of $\tau_{T_1} : J \subset \mathbb{P}^{15} \to J \subset \mathbb{P}^{15}$ when $T_1 \in J[4]$. We do this via the following proposition.

Proposition 4.2.5. *Suppose $T_1 \in J[4]$. Given the coordinates of $T_1 \in J \subset \mathbb{P}^{15}_{\{k_{ij},b_i\}}$, we can compute the following composition of morphisms:*

$$\Psi : J \subset \mathbb{P}^{15}_{\{k_{ij},b_i\}} \xrightarrow{\tau_{T_1}} J \subset \mathbb{P}^{15}_{\{k_{ij},b_i\}} \xrightarrow{proj} \mathbb{P}^9_{k_{ij}}.$$

Proof. Let $T = 2T_1 \in J[2]$. Recall that we let M_T denote the action of translation by T on $\mathcal{K} \subset \mathbb{P}^3$. Then for any $P \in J$, we have $k_i(P+T) =$

$\sum_{j=1}^{4}(M_T)_{ij}k_j(P)$ projectively, as a vector of length 4, and the following equalities hold projectively, as a vector of length 10,

$$\begin{aligned}
&k_{ij}(P+T_1)\\
&= k_i(P+T_1)k_j(P+T_1)\\
&= k_i(P+T_1)k_j(\tau_T(P-T_1))\\
&= k_i(P+T_1)\cdot\sum_{l=1}^{4}(M_T)_{jl}k_l(P-T_1)\\
&= \sum_{l=1}^{4}(M_T)_{jl}k_l(P-T_1)k_i(P+T_1).
\end{aligned}$$

By Theorem 1.3.5, there exists a 4×4 matrix of bilinear forms $\phi_{ij}(P,T_1)$, with explicit formula, that is projectively equal to the matrix $k_i(P-T_1)k_j(P+T_1)$. Since we have an explicit formula for M_T in [CF96, Chapter 3, Section 2], we can partially compute the linear isomorphism τ_{T_1}:

$$\Psi : J \subset \mathbb{P}^{15}_{\{k_{ij},b_i\}} \xrightarrow{\tau_{T_1}} J \subset \mathbb{P}^{15}_{\{k_{ij},b_i\}} \xrightarrow{proj} \mathbb{P}^{9}_{k_{ij}},$$

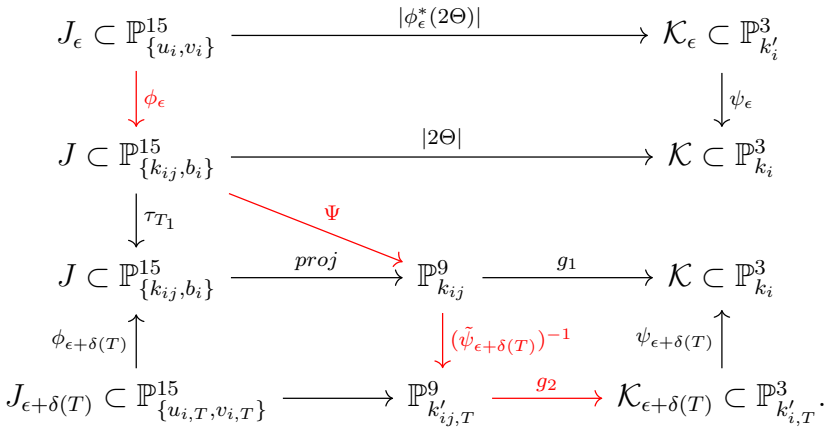
as required.

□

Remark 4.2.6. Suppose $2T_1 = T \in J[2]$. From the doubling formula on $\mathcal{K}$ as in [Fly93, Appendix C], we can compute the coordinates of the image of T_1 on $\mathcal{K} \subset \mathbb{P}^3$ from the coordinates of the image of T on $\mathcal{K} \subset \mathbb{P}^3$. This gives the 10 even coordinates, $k_{ij}(T_1)$ and we can solve for the odd coordinates by the 72 defining equations of J given in Theorem 1.3.2. Note that by Lemma 4.2.4, we know the field of definition of T_1 is contained in the composition of the field of definition of ϕ_ϵ and $\phi_{\epsilon+\delta(T)}$. Hence, we can compute this field explicitly which helps with the point search using MAGMA.

Consider $T \in J[2]$ with $T_1 \in J[4]$ such that $2T_1 = T$. We follow the discussion in Section 4.2.2 for $\epsilon+\delta(T)$ and compute a similar diagram as (4.2.1) for $\epsilon + \delta(T)$. Suppose we embed $\mathcal{K}_{\epsilon+\delta(T)}$ in $\mathbb{P}^3$ with coordinates $k'_{1,T},...,k'_{4,T}$ and embed $J_{\epsilon+\delta(T)}$ in $\mathbb{P}^{15}$ with coordinates $u_{0,T},...,u_{9,T},v_{1,T},...,v_{6,T}$. Let $k'_{ij,T} =$

$k'_{i,T}k'_{j,T}$. Consider the commutative diagram below:



(4.2.2)

Recall Proposition 4.2.5 explains how Ψ can be explicitly computed and the composition of the red morphisms in (4.2.2) is defined over K by Lemma 4.2.4. Let D_T be the pull back on J_ϵ via the red morphisms in (4.2.2) of the hyperplane section given by $k'_{1,T} = 0$. This implies that D_T is a K-rational divisor on J_ϵ representing the class of $\phi_\epsilon^*(\tau_{T_1}^*(2\Theta))$. Moreover, the pull back on J_ϵ via $J_\epsilon \subset \mathbb{P}^{15}_{\{u_i,v_i\}} \xrightarrow{\phi_\epsilon} J \subset \mathbb{P}^{15}_{\{k_{ij,b_i}\}} \xrightarrow{\Psi} \mathbb{P}^9_{kij} \xrightarrow{(\tilde{\psi}_{\epsilon+\delta(T)})^{-1}} \mathbb{P}^9_{k'_{ij,T}}$ of the hyperplane section given by $k'_{11,T} = 0$ is $2D_T$.

We now apply the above discussion with $T = P, Q, R, S$ and get the K-rational divisors D_P, D_Q, D_R, D_S on J_ϵ described in Remark 4.1.3 as required.

Remark 4.2.7. From the above discussion and the discussion in Section 4.2.2, the K-rational functions f_P, f_Q, f_R, f_S in the formula for the Cassels-Tate pairing in Theorem 4.1.4 are quotients of linear forms in the coordinates of the ambient space of $J_\epsilon \subset \mathbb{P}^{15}$. In particular, they have the same denominator.

4.3 Obstruction Map

In this section, we give the explicit formula for the obstruction map $\mathrm{Ob} : H^1(G_K, J[2]) \to \mathrm{Br}(K)$ defined in Section 3.3.2. Recall we have explicit formula for $M_T \in \mathrm{GL}_4(K)$ given in [CF96, Chapter 3 Section 2], which represents the action of translation by $T \in J[2]$ on the Kummer surface $\mathcal{K} \subset \mathbb{P}^3$. In particular, we define $c_P, c_Q, c_R, c_S \in K$ such that $M_P^2 = c_P I, M_Q^2 = c_Q I, M_R^2 = c_R I$, and $M_S^2 = c_S I$ with P, Q, R, S a set of generators for $J[2]$ satisfying the Weil pairing matrix (4.1.1). Also, $[M_P, M_Q] = [M_R, M_S] = -I$ and the commutators of the other pairs are trivial. Consider $\epsilon \in \mathrm{Sel}^2(J)$ that corresponds to $(a, b, c, d) \in (K^*/(K^*)^2)^4$ as in Section 4.1.1. By Proposition 3.3.8, we know that a representation of $\mathrm{Ob}(\epsilon)$ is the enveloping algebra for $\mathbf{\Theta}_\epsilon$ which is naturally given as $(c_P a, c_Q b) \otimes (c_R c, c_S d)$ from the discussion in Section 4.2.1. From

this observation and the formula for the obstruction map in the case of elliptic curves, we conjectured that such formula exists for any element in $H^1(G_K, J[2])$. This is proved in the following theorem.

Theorem 4.3.1. *Let J be the Jacobian variety of a genus two curve defined over a field K with $char(K) \neq 2$. Suppose all points in $J[2]$ are defined over K. For $\epsilon \in H^1(G_K, J[2])$, represented by $(a, b, c, d) \in (K^*/(K^*)^2)^4$ as in Section 4.1.1, the obstruction map $Ob : H^1(G_K, J[2]) \to Br(K)$ sends ϵ to the class of the tensor product of two quaternion algebras:*

$$Ob(\epsilon) = (c_P a, c_Q b) + (c_R c, c_S d).$$

Proof. Let $N_P = \frac{1}{\sqrt{c_P}} M_P, N_Q = \frac{1}{\sqrt{c_Q}} M_Q, N_R = \frac{1}{\sqrt{c_R}} M_R, N_S = \frac{1}{\sqrt{c_S}} M_S \in \mathrm{GL}_4(\bar{K})$. Then N_P is a normalized representation in $\mathrm{GL}_4(\bar{K})$ of $[M_P] \in \mathrm{PGL}_4(K)$. Similar statements are true for Q, R, S. Notice that $N_P^2 = N_Q^2 = N_R^2 = N_S^2 = I$. So there is a uniform way of picking a representation in $\mathrm{GL}_4(\bar{K})$ for the translation induced by $\alpha_1 P + \alpha_2 Q + \alpha_3 R + \alpha_4 S$ for $\alpha_i \in \mathbb{Z}$, namely $N_P^{\alpha_1} N_Q^{\alpha_2} N_R^{\alpha_3} N_S^{\alpha_4}$.

Since $\epsilon \in H^1(K, J[2])$ is represented by $(a, b, c, d) \in (K^*/K^{*2})^4$ as in Section 4.1.1 and P, Q, R, S satisfy the Weil pairing matrix (4.1.1), a cocycle representation of ϵ is:

$$\sigma \mapsto \tilde{b}_\sigma P + \tilde{a}_\sigma Q + \tilde{d}_\sigma R + \tilde{c}_\sigma S,$$

where for each element $x \in K^*/(K^*)^2$, we define $\tilde{x}_\sigma \in \{0, 1\}$ such that $(-1)^{\tilde{x}_\sigma} = \sigma(\sqrt{x})/\sqrt{x}$.

Now consider the following commutative diagram of cochains:

$$\begin{array}{ccccc} C^1(G_K, \mathbb{G}_m) & \longrightarrow & C^1(G_K, \mathrm{GL}_4) & \longrightarrow & C^1(G_K, \mathrm{PGL}_4) \\ \downarrow d & & \downarrow d & & \downarrow d \\ C^2(G_K, \mathbb{G}_m) & \longrightarrow & C^2(G_K, \mathrm{GL}_4) & \longrightarrow & C^2(G_K, \mathrm{PGL}_4). \end{array}$$

Define $N_\sigma = N_P^{\tilde{b}_\sigma} N_Q^{\tilde{a}_\sigma} N_R^{\tilde{d}_\sigma} N_S^{\tilde{c}_\sigma}$, we have

$$\begin{array}{ccc} H^1(K, J[2]) & \to & H^1(G_K, \mathrm{PGL}_4) \\ (a, b, c, d) & \mapsto & (\sigma \mapsto [N_\sigma]). \end{array}$$

Then $(\sigma \mapsto [N_\sigma]) \in C^1(G_K, \mathrm{PGL}_4)$ lifts to $(\sigma \mapsto N_\sigma) \in C^1(G_K, \mathrm{GL}_4)$ which is then mapped to

$$((\sigma, \tau) \mapsto (N_\tau)^\sigma N_{\sigma\tau}^{-1} N_\sigma) \in C^2(G_K, \mathrm{GL}_4).$$

Note that $N_P^\sigma = (\frac{1}{\sqrt{c_P}}M_P)^\sigma = \frac{1}{\sigma(\sqrt{c_P})}M_P = \frac{\sqrt{c_P}}{\sigma(\sqrt{c_P})}N_P = (-1)^{(\tilde{c_P})_\sigma}N_P$, treating c_P in $K^*/(K^*)^2$. Similar results also hold for Q, R, S. Observe that for any $x \in K^*/(K^*)^2, \sigma, \tau \in G_K$, we have $\tilde{x}_\sigma - \tilde{x}_{\sigma\tau} + \tilde{x}_\sigma$ is equal to 0 or 2. Since $N_P^2 = N_Q^2 = N_R^2 = N_S^2 = I$, $[N_P, N_Q] = [N_R, N_S] = -I$ and the commutators of the other pairs are trivial, we have

$$\begin{aligned}
&(N_\tau)^\sigma N_{\sigma\tau}^{-1} N_\sigma \\
=&(N_P^{\tilde{b}_\tau} N_Q^{\tilde{a}_\tau} N_R^{\tilde{d}_\tau} N_S^{\tilde{c}_\tau})^\sigma N_S^{-\tilde{c}_{\sigma\tau}} N_R^{-\tilde{d}_{\sigma\tau}} N_Q^{-\tilde{a}_{\sigma\tau}} N_P^{-\tilde{b}_{\sigma\tau}} N_P^{\tilde{b}_\sigma} N_Q^{\tilde{a}_\sigma} N_R^{\tilde{d}_\sigma} N_S^{\tilde{c}_\sigma} \\
=&(-1)^{(\tilde{c_P})_\sigma \cdot \tilde{b}_\tau} \cdot (-1)^{(\tilde{c_Q})_\sigma \cdot \tilde{a}_\tau} \cdot (-1)^{(\tilde{c_R})_\sigma \cdot \tilde{d}_\tau} \cdot (-1)^{(\tilde{c_S})_\sigma \cdot \tilde{c}_\tau} \\
&\cdot N_P^{\tilde{b}_\tau} N_Q^{\tilde{a}_\tau} N_R^{\tilde{d}_\tau} N_S^{\tilde{c}_\tau} N_S^{-\tilde{c}_{\sigma\tau}} N_R^{-\tilde{d}_{\sigma\tau}} N_Q^{-\tilde{a}_{\sigma\tau}} N_P^{-\tilde{b}_{\sigma\tau}} N_P^{\tilde{b}_\sigma} N_Q^{\tilde{a}_\sigma} N_R^{\tilde{d}_\sigma} N_S^{\tilde{c}_\sigma} \\
=&(-1)^{(\tilde{c_P})_\sigma \cdot \tilde{b}_\tau} \cdot (-1)^{(\tilde{c_Q})_\sigma \cdot \tilde{a}_\tau} \cdot (-1)^{(\tilde{c_R})_\sigma \cdot \tilde{d}_\tau} \cdot (-1)^{(\tilde{c_S})_\sigma \cdot \tilde{c}_\tau} \\
&\cdot N_P^{\tilde{b}_\tau} N_Q^{\tilde{a}_\tau} N_Q^{-\tilde{a}_{\sigma\tau}} N_P^{-\tilde{b}_{\sigma\tau}} N_P^{\tilde{b}_\sigma} N_Q^{\tilde{a}_\sigma} \cdot N_R^{\tilde{d}_\tau} N_S^{\tilde{c}_\tau} N_S^{-\tilde{c}_{\sigma\tau}} N_R^{-\tilde{d}_{\sigma\tau}} N_R^{\tilde{d}_\sigma} N_S^{\tilde{c}_\sigma} \\
=&(-1)^{(\tilde{c_P})_\sigma \cdot \tilde{b}_\tau} \cdot (-1)^{(\tilde{c_Q})_\sigma \cdot \tilde{a}_\tau} \cdot (-1)^{(\tilde{c_R})_\sigma \cdot \tilde{d}_\tau} \cdot (-1)^{(\tilde{c_S})_\sigma \cdot \tilde{c}_\tau} \cdot (-1)^{\tilde{b}_\tau \cdot \tilde{a}_\sigma} \cdot (-1)^{\tilde{d}_\tau \cdot \tilde{c}_\sigma} \cdot I.
\end{aligned}$$

On the other hand, $(c_P, c_Q) \otimes (c_R, c_S)$ is isomorphic to $< M_P, M_Q, M_R, M_S >= \mathrm{Mat}_4(K)$ which represents the identity element in the Brauer group. Hence, by Proposition 1.4.11, we have

$$(c_P a, c_Q b) + (c_R c, c_S d) = (a, b) + (c, d) + (c_P, b) + (c_Q, a) + (c_R, d) + (c_S, c).$$

From Proposition 1.4.13, we have $\mathrm{Br}(K) \cong H^2(G_K, \bar{K}^*)$. By Remark 1.4.16, we know the cocycle representation of the class of a quaternion algebra (α, β) in $\mathrm{Br}(K)$ is precisely $(\sigma, \tau) \mapsto (-1)^{\tilde{\alpha}_\sigma \cdot \tilde{\beta}_\tau}$, treating $\alpha, \beta \in K^*/(K^*)^2$. Therefore, a cocycle representation of $(a, b) + (c, d) + (c_P, b) + (c_Q, a) + (c_R, d) + (c_S, c) \in \mathrm{Br}(K) \cong H^2(G_K, \bar{K}^*)$ sends (σ, τ) to

$$(-1)^{(\tilde{c_P})_\sigma \cdot \tilde{b}_\tau} \cdot (-1)^{(\tilde{c_Q})_\sigma \cdot \tilde{a}_\tau} \cdot (-1)^{(\tilde{c_R})_\sigma \cdot \tilde{d}_\tau} \cdot (-1)^{(\tilde{c_S})_\sigma \cdot \tilde{c}_\tau} \cdot (-1)^{\tilde{b}_\tau \cdot \tilde{a}_\sigma} \cdot (-1)^{\tilde{d}_\tau \cdot \tilde{c}_\sigma},$$

for all $\sigma, \tau \in G_K$ as required.

□

Remark 4.3.2. Theorem 4.3.1 generalizes the theorem in the elliptic curve case, which was done by O'Neil in [O'N02, Proposition 3.4], and later refined by Clark in [Cla05, Theorem 6].

4.4 Prime Bound

Suppose all points in $J[2]$ are defined over K. In Theorem 4.1.4, we proved that the Cassels-Tate pairing of $\epsilon, \eta \in \mathrm{Sel}^2(J)$, with η corresponding to $(a, b, c, d) \in$

$(K^*/(K^*)^2)^4$ as in Section 4.1.1, has the formula

$$\langle \epsilon, \eta \rangle_{CT} = \prod_v (f_p(P_v), b)_v (f_Q(P_v), a)_v (f_R(P_v), d)_v (f_S(P_v), c)_v.$$

Recall that $(\ ,\ )_v$ denotes the Hilbert Symbol for a given place v of K and P, Q, R, S are generators for $J[2]$ satisfying the Weil pairing matrix (4.1.1). Let $(J_\epsilon, [2] \circ \phi_\epsilon)$ denote the 2-covering of J corresponding to ϵ. By Remark 4.2.7, we know f_P, f_Q, f_R, f_S are computable as quotients of two linear forms with the same denominator, in the coordinates of the ambient space of $J_\epsilon \subset \mathbb{P}^{15}$, denoted by $x_1, ..., x_{16}$ in this section. Also P_v is any local point on J_ϵ avoiding the zeros and poles of f_P, f_Q, f_R, f_S.

In this section, we show that the above formula for the Cassels-Tate pairing is actually always a finite product, as mentioned in Remark 4.1.5. In particular, there exists a computable bound for each pair of (ϵ, η), which depends on f_S, f_Q, f_R, f_S, such that for a place of K whose norm is a power of a prime above that bound, the local Cassels-Tate pairing between ϵ and η is trivial.

4.4.1 Statement of the problem

Let $\mathcal{O}_K$ be the ring of integers for the number field K. By rescaling the variables, we assume the genus two curve is defined by $y^2 = f(x) = f_6 x^6 + ... + f_0$ where f is defined over $\mathcal{O}_K$.

Recall we have $S = \{\text{places of bad reduction for } \mathcal{C}\} \cup \{\text{places dividing } 2\} \cup \{\text{infinite places}\}$. For the Selmer element $\eta = (a, b, c, d) \in (K^*/(K^*)^2)^4$, we have $a, b, c, d \in K(S, 2)$ by Remark 4.1.1. Hence, outside S, the second arguments of the Hilbert symbols in the formula for $\langle \epsilon, \eta \rangle_{CT}$ have valuation 0. By the definition of the Hilbert symbol in Section 1.4.4 and Lemma 1.4.18, it suffices to find a finite set S_1, a subset of places of K containing S, such that outside S_1 the first arguments of the Hilbert symbols in the formula for $\langle \epsilon, \eta \rangle_{CT}$ also have valuation 0.

The first arguments of the Hilbert symbols in the formula for $\langle \epsilon, \eta \rangle_{CT}$ are $f_P(P_v)$, $f_Q(P_v)$, $f_R(P_v)$ or $f_S(P_v)$, where f_P, f_Q, f_R, f_S can be computed as the quotients of two linear forms in $\mathbb{P}^{15}$ with the denominators being the same, as explained in Remark 4.2.7. Since we know that the Cassels-Tate pairing is independent of the choice of the local points P_v as long as it avoids all the zeros and poles, it suffices to find a finite set of places S_1 containing S such that there exists at least one local point P_v on J_ϵ with which the values of the quotients of the linear forms all have valuation 0 for all v outside S_1. So the following is the statement of the problem that we need to solve.

Problem 4.4.1. Let $l_1, ...l_n$ be n linear forms in variables $x_1, ..., x_{16}$ with coefficients in $\mathcal{O}_K$, for some integer $n \geq 2$. Does there exist a finite set S_1 of places

of K containing S that depends only on n, coefficients of $l_1, ..., l_n$, and $f_0, ..., f_6$, such that for any place v of K outside S_1, there exists $Q_v \in J_\epsilon(\mathbb{Q}_v) \subset \mathbb{P}^{15}_{x_i}$ such that $l_i/l_1(Q_v)$ has valuation 0, for all $i = 2, ...n$?

4.4.2 Reduction of the problem

We now give a solution to Problem 4.4.1. The idea is to first reduce the problem to the residue field.

Suppose $(a_1, ..., a_6)$ represents the image of ϵ in $L^*/(L^*)^2K^*$ with $L = K[x]/(f)$ as described in Section 1.10.1. By Theorem 1.11.1 and Remark 1.11.2, we have an explicit formula for the linear isomorphism ϕ_ϵ

$$J_\epsilon \subset \mathbb{P}^{15} \xrightarrow{\phi_\epsilon} J \subset \mathbb{P}^{15},$$

which is defined over $K(\sqrt{a_1}, ..., \sqrt{a_6})$ and $(J_\epsilon, [2] \circ \phi_\epsilon)$ is the 2-covering of J corresponding to ϵ. Let $\epsilon = (s_1, s_2, s_3, s_4) \in (K^*/(K^*)^2)^4$ as in Section 4.1.1, we showed $(s_1, s_2, s_3, s_4) = (a_1a_2, a_1a_3, a_4a_5, a_4a_6) \in (K^*/(K^*)^2)^4$. It can be checked that $K(\sqrt{a_1a_6}, ..., \sqrt{a_6a_6}) = K(\sqrt{s_1}, \sqrt{s_2}, \sqrt{s_3}, \sqrt{s_4})$ and we let K' denote this field. Since $(a_1a_6, ..., a_6a_6)$ also represents the image of ϵ in $L^*/(L^*)^2K^*$, we have an explicit formula for the linear isomorphism ϕ_ϵ, represented by $M_\epsilon \in \mathrm{GL}_{16}(K')$. Note we can assume that all entries of M_ϵ are in $\mathcal{O}_{K'}$, the ring of integers of K'.

Notation 4.4.2. Let K be a local field with valuation ring $\mathcal{O}_K$ and residue field k. Let $X \subset \mathbb{P}^N$ be a variety defined over K and $I(X) \subset K[x_0, ..., x_N]$ be the ideal of X. Then the reduction of X, denoted by $\bar{X}$, is the variety defined by the polynomials $\{\bar{f} : f \in I(X) \cap \mathcal{O}_K[x_0, ..., x_N]\}$. Here $\bar{f}$ for a polynomial f with coefficients defined over $\mathcal{O}_K$ denotes the same polynomial with coefficients in the residue field k.

Remark 4.4.3. Note that the definition of the reduction of a variety $X \subset \mathbb{P}^N$ defined over a local field K in Notation 4.4.2 is equivalent to taking the special fibre of the closure of X in $\mathbb{P}^N_S$, where $S = \operatorname{Spec} \mathcal{O}_K$.

Fix a place $v \notin S$ of K and suppose it is above the prime p. We now treat J, J_ϵ and $\mathcal{C}$ as varieties defined over the local field K_v. Let $\mathcal{O}_v$ denote the valuation ring of K_v and $\mathbb{F}_q$ denote its residue field, where q is some power of p. It can be shown that $\bar{J}$ is also an abelian variety as the defining equations of J are defined over $\mathcal{O}_v$ and are derived algebraically in terms of the coefficients of the defining equation of the genus two curve $\mathcal{C}$ by Theorem 1.3.2. In fact, $\bar{J}$ is the Jacobian variety of $\bar{\mathcal{C}}$, the reduction of $\mathcal{C}$. We have the following two lemmas.

Lemma 4.4.4. *Let X and Y be varieties in $\mathbb{P}^N$ defined over a local field K, and are isomorphic via a matrix $M \in GL_{N+1}(\mathcal{O}_K)$ where $\mathcal{O}_K$ is the valuation ring of K. Then their reductions are isomorphic over $\mathbb{F}_q$.*

Proof. Let $I = I(X), J = I(Y)$. Denote $I' = I \cap \mathcal{O}_K[x_0, ..., x_N], J' = J \cap \mathcal{O}_K[x_0, ..., x_N]$ and $\bar{I'} = \{\bar{f} : f \in I'\}$ and $\bar{J'} = \{\bar{f} : f \in J'\}$. Let $\bar{M}$ denote M over the residue field $\mathbb{F}_q$, we have $\bar{M}$ is a well-defined invertible matrix in $\mathrm{GL}_{N+1}(\mathbb{F}_q)$. Also we have $I = M^*J := \{f \circ M : f \in J\}$ as M is an isomorphism $X \to Y$. Hence, $I' = I \cap \mathcal{O}_K[x_0, ..., x_N] = (M^*J) \cap \mathcal{O}_K[x_0, ..., x_N] = M^*(J \cap \mathcal{O}_K[x_0, ..., x_N]) = M^*J'$. This implies that $\bar{I'} = \bar{M}^*\bar{J'}$ which means that $\bar{M}$ is a morphism $\bar{X} \to \bar{Y}$. Hence, $\bar{M}$ is indeed an isomorphism $\bar{X} \to \bar{Y}$ as required.

□

Lemma 4.4.5. *Let L be a finite extension of a local field K, with their valuation rings denoted by $\mathcal{O}_L, \mathcal{O}_K$ respectively. For an ideal $I \subset K[x_0, ..., x_N]$, we have*

$$(I \otimes L) \cap \mathcal{O}_L[x_0, ..., x_N] = (I \cap \mathcal{O}_K[x_0, ..., x_N]) \otimes_{\mathcal{O}_K} \mathcal{O}_L.$$

Proof. We observe that $(I \cap \mathcal{O}_K[x_0, ..., x_N]) \otimes_{\mathcal{O}_K} \mathcal{O}_L \subset (I \otimes L) \cap \mathcal{O}_L[x_0, ..., x_N]$ is immediate. It suffices to prove

$$(I \otimes L) \cap \mathcal{O}_L[x_0, ..., x_N] \subset (I \cap \mathcal{O}_K[x_0, ..., x_N]) \otimes_{\mathcal{O}_K} \mathcal{O}_L.$$

Since $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module, we let $b_1, ..., b_m$ be a free basis for $\mathcal{O}_L$ as $\mathcal{O}_K$-module. Note that they are also basis for L as a K-module. Moreover, we know that $\sum_{i=1}^m x_i b_i \in \mathcal{O}_L$ for some $x_i \in K$ if and only if $x_i \in \mathcal{O}_K$ for any i. Suppose $v \in (I \otimes L) \cap \mathcal{O}_L[x_0, ..., x_N]$. Since $v \in (I \otimes L)$, we get $v = \sum_{i=1}^m v_i b_i$ for some $v_i \in I$. Since $v \in \mathcal{O}_L[x_0, ..., x_N]$, we get that $v_i \in \mathcal{O}_K[x_0, ..., x_N]$. Hence, $v \in (I \cap \mathcal{O}_K[x_0, ..., x_N]) \otimes_{\mathcal{O}_K} \mathcal{O}_L$ as required.

□

Now fix a place v' of K' above the place v of K. Let $O_{v'}$ and $\mathbb{F}_{q^r}$ denote the valuation ring and the residue field of $K'_{v'}$. We treat J, J_ϵ as varieties defined over $K'_{v'}$ and apply Lemma 4.4.4. By Lemma 4.4.5, we know that the reductions of J, J_ϵ treated as varieties defined over $K'_{v'}$ is the same as the reductions of J, J_ϵ as varieties over K_v, but treated as varieties defined over $\mathbb{F}_{q^r}$. Hence, as long as v' does not divide $\det M_\epsilon \in \mathcal{O}_{K'}$, the following diagram commutes and $\bar{M}_\epsilon$ is a well defined linear isomorphism defined over the residue field $\mathbb{F}_{q^r}$ between the two varieties defined over $\mathbb{F}_q$: $\bar{J}_\epsilon \to \bar{J}$.

$$\begin{array}{ccc} J_\epsilon \subset \mathbb{P}^{15} & \xrightarrow{M_\epsilon} & J \subset \mathbb{P}^{15} \\ \downarrow \text{reduction} & & \downarrow \text{reduction} \\ \bar{J}_\epsilon \subset \mathbb{P}^{15} & \xrightarrow{\bar{M}_\epsilon} & \bar{J} \subset \mathbb{P}^{15}, \end{array}$$

where $\bar{M}_\epsilon$ denotes the matrix M_ϵ over the residue field $\mathbb{F}_{q^r}$.

This linear isomorphism $\bar{M}_\epsilon$ implies that $\bar{J}_\epsilon$ is smooth whenever $\bar{J}$ is and in which case, $\bar{J}_\epsilon$ is a twist of $\bar{J}$. It in fact is a principal homogeneous space of $\bar{J}$. Indeed, the surjectivity of the natural map $\mathrm{Gal}(K'_{v'}/K_v) \to \mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ shows that $M(M^{-1})^\sigma = \tau_{P_\sigma}$ for all $\sigma \in \mathrm{Gal}(K'_{v'}/K_v)$ implies that $\bar{M}(\bar{M}^{-1})^{\bar{\sigma}} = \tau_{\bar{P}_{\bar{\sigma}}}$ for all $\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$. We know any principal homogeneous space of $\bar{J}$ over a finite field has a point by [Lan56, Theorem 2] and so is trivial by Corollary 1.5.6. Therefore, there exists an isomorphism $\psi\colon \bar{J}_\epsilon \xrightarrow{\psi} \bar{J}$ defined over $\mathbb{F}_q$. Hence, as long as $v \notin S$ and v does not divide $N_{K'/K}(\det M_\epsilon)$, $\bar{J}_\epsilon$ has the same number of $\mathbb{F}_q$-points as $\bar{J}$. By the Hasse-Weil bound, we know the number of $\mathbb{F}_q$-points on $\mathcal{C}$ is bounded below by $q-1-4\sqrt{q}$. Since we can represent points on $\bar{J}$ by pairs of points on $\bar{\mathcal{C}}$ and this representation is unique other than the identity point on $\bar{J}$, as discussed in Section 1.2.2. The number of $\mathbb{F}_q$-points on $\bar{J}$ is bounded below by $(q-1-4\sqrt{q})(q-3-4\sqrt{q})/2$.

On the other hand, we assume that the coefficients of l_i are in $\mathcal{O}_K$ by scaling, for all $i = 1, ..., n$. Fix a place v of K that does not divide all the coefficients of l_i, for any $i = 1, ..., n$. Let H_i be the hyperplane defined by the linear form l_i and $\bar{H}_i$ be its reduction, which is a hyperplane defined over the residue field $\mathbb{F}_q$, We need to bound the number of $\mathbb{F}_q$-points of $\bar{J}_\epsilon$ that lie on one of the hyperplanes $\bar{H}_i$. Let r_i be the number of irreducible components of $\bar{J}_\epsilon \cap \bar{H}_i$. By [Har77, Chapter 1, Theorem 7.2(Projective Dimension Theorem) and Theorem 7.7], we know that each irreducible component C^i_j of $\bar{J}_\epsilon \cap \bar{H}_i$, where $j = 1, ..., r_i$, is a curve and the sum of degrees of all the irreducible components counting intersection multiplicity is $\deg \bar{J}_\epsilon = 32$. Let $d^i_j = \deg C^i_j$, we get $\sum_{j=1}^{r_i} d^i_j \leq 32$ for all i. This implies that for a hyperplane that does not contain C^i_j, the number of intersections of C^i_j and the hyperplane counting multiplicity is d^i_j. Suppose each irreducible component C^i_j is contained in $\mathbb{P}^{N^i_j}$ but not in $\mathbb{P}^{N^i_j-1}$ (i.e. it is not contained in any hyperplane in $\mathbb{P}^{N^i_j}$), for some $N^i_j \in \mathbb{N}$ with $N^i_j \leq 15$. Note, the number of hyperplanes in $\mathbb{P}^N$ over $\mathbb{F}_q$ is $\frac{q^{N+1}-1}{q-1} = \sum_{i=0}^{N} q^i$, for all $N \in \mathbb{N}$. Also, each $\mathbb{F}_q$-point in $\mathbb{P}^N$ lies on $\sum_{i=0}^{N-1} q^i$ many hyperplanes, we get the number of $\mathbb{F}_q$-points of $\bar{J}_\epsilon$ that lie on one of the hyperplanes $\bar{H}_i, i = 1, ..., n$, is no more than

$$\sum_{i=1}^{n}\sum_{j=1}^{r_i} \frac{d^i_j \cdot \sum_{k=0}^{N^i_j} q^k}{\sum_{k=0}^{N^i_j-1} q^k} \leq \sum_{i=1}^{n}\sum_{j=1}^{r_i} d^i_j \cdot (q+1),$$

which is bounded above by $32(q+1)\cdot n$.

To sum up, if v is a place of K above the prime p such that $v \notin S$, v does not divide $N_{K'/K}(\det M_\epsilon)$ or all the coefficients of l_i for some i and $(q-1-4\sqrt{q})(q-3-4\sqrt{q})/2 > 32(q+1)\cdot n$, we have a smooth $\mathbb{F}_q$-point on $\bar{J}_\epsilon$ which by Hensel's Lemma [HS00, Exercise C.9(c)] lifts to the point Q_v as required. Recall that q is the size of the residue field of K_v and so is a power of p. We know there exists a bound $N' \in \mathbb{N}$ that depends on n such that any $x > N'$, $(x-1-4\sqrt{x})(x-3-4\sqrt{x})/2 > 32(x+1)\cdot n$. Hence, the finite set S_1 can be taken to be the set $S \cup \{\text{places dividing } N_{K'/K}(\det M_\epsilon)\} \cup$

{places dividing all the coefficients of l_i for some i}$\cup${places above primes less than N$'$}. Therefore, the answer to Problem 4.4.1 is yes and the bound N can be the maximum prime p that divides the norm of some element in S_1.

Remark 4.4.6. To show the formula for the Cassels-Tate pairing in Theorem 4.1.4 is always a finite product, we need to solve Problem 4.4.1 with $n = 5$. Note for any $x > 500$, we have $(x-1-4\sqrt{x})(x-3-4\sqrt{x})/2 > 32(x+1)\cdot 5$. Suppose all entries of M_ϵ are in $\mathcal{O}_{K'}$ and f is defined over $\mathcal{O}_K$, the set S_1 can be taken to be {places of bad reduction for $\mathcal{C}$}$\cup${places dividing 2}$\cup${infinite places}$\cup$ {places dividing $N_{K'/K}(\det M_\epsilon)$} $\cup$ {places dividing all the coefficients of the denominator or the numerator of f_P, f_Q, f_R or f_S}$\cup${places above primes less than 500}. By the discussion above, the local Cassels-Tate pairing between $\epsilon, \eta \in \mathrm{Sel}^2(J)$ is trivial for any prime of K above the maximum prime p that divides the norm of some element of S_1. Hence, the formula for the Cassels-Tate is indeed always a finite product.

Note that the set S_1 in Remark 4.4.6 is under the assumptions that all entries of M_ϵ are in $\mathcal{O}_{K'}$ and f is defined over $\mathcal{O}_K$ where the genus two curve is defined by $y^2 = f(x)$. We give the following remarks on some practical issues and simplification.

Remark 4.4.7.

(i) We can always rescale y to make f defined over $\mathcal{O}_K$.

(ii) In the case where not all entries of M_ϵ are in $\mathcal{O}_{K'}$ and $K = \mathbb{Q}$, we look for $n \in \mathbb{Z}$ such that all entries of nM_ϵ are in $\mathcal{O}_{K'}$. Suppose $K' = \mathbb{Q}(x)$ with $x \in \mathcal{O}_{K'}$ and $[K' : \mathbb{Q}] = m$. For each $a \in K'$, define $d(a)$ to be the least common multiple of the denominators of $c_0, ..., c_{m-1}$, where $a = \sum_{i=0}^{m-1} c_i x^i$ and $c_i \in \mathbb{Q}$ in the simplest form. Then $d(a)\cdot a \in \mathcal{O}_{K'}$ and we can take n to be the least common multiple of $d((M_\epsilon)_{11}), d((M_\epsilon)_{12}), ..., d((M_\epsilon)_{44})$. This implies we can replace the subset {places dividing $N_{K'/K}(\det M_\epsilon)$} in the definition of S_1 by S' which is the set of all primes dividing n or the numerator of $N_{K'/\mathbb{Q}}(\det M_\epsilon)$. Note that this method is far from optimal and might include a lot more primes than needed. For example, one possible improvement is to pick a more suitable integral basis for K'. However, it does not require any number field computation and is a practical method as the local Cassels-Tate pairing is fast to compute.

(iii) In the case where $K = \mathbb{Q}$, we can always make the linear forms primitive by scaling. Therefore, in this case, the subset {places dividing all the coefficients of the denominator or the numerator of f_P, f_Q, f_R or f_S} of S_1 is empty.

4.5 Algorithm and Worked Example

In this section, we describe an algorithm for computing the Cassels-Tate pairing on $\mathrm{Sel}^2(J) \times \mathrm{Sel}^2(J)$ using the formula in Theorem 4.1.4, where J is the Jacobian variety of a genus two curve defined over a number field K such that all points in $J[2]$ are defined over K. Then we will apply this algorithm in a worked example. Note that this algorithm in theory works over any number field, but we have only computed examples in the case $K = \mathbb{Q}$.

4.5.1 Description of the algorithm

Start with a genus two curve $\mathcal{C}$ with the following defining equation which we can assume to be defined over $\mathcal{O}_K$ by rescaling y:

$$\mathcal{C} : y^2 = f(x) = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0,$$

with all roots of f defined over K which implies that all points in $J[2]$ are over K by Remark 1.2.1. We denote the roots of f by $\omega_1, ..., \omega_6$ and let the generators of $J[2]$ be

$$P = \{(\omega_1, 0), (\omega_2, 0)\}, \quad Q = \{(\omega_1, 0), (\omega_3, 0)\},$$
$$R = \{(\omega_4, 0), (\omega_5, 0)\}, \quad S = \{(\omega_4, 0), (\omega_6, 0)\}.$$

We know that they satisfy the Weil pairing matrix (4.1.1). Let $\delta : J(K)/2J(K) \to H^1(G_K, J[2])$ denote the connecting map induced by the short exact sequence $0 \to J[2] \to J \xrightarrow{2} J \to 0$ and let $\delta(P), \delta(Q), \delta(R), \delta(S)$ denote the images of $[P], [Q], [R], [S] \in J(K)/2J(K)$ in $H^1(G_K, J[2])$.

For $\epsilon, \eta \in \mathrm{Sel}^2(J)$, we give an algorithm for computing $\langle \epsilon, \eta \rangle_{CT}$.

- Step 1: Compute the image of ϵ, η in $(K^*/(K^*)^2)^4$. Note that MAGMA gives their images in $(L^*/(L^*)^2K^*)$ where $L = K[x]/(f)$ as discussed in Remark 3.2.8. Follow the discussion in Section 4.1.1, we can then find the corresponding elements in $(K^*/(K^*)^2)^4$.

- Step 2: By the explicit formula for the Cassels map in Remark 1.10.3, compute $\delta(P), \delta(Q), \delta(R), \delta(S) \in \mathrm{Sel}^2(J) \subset H^1(G_K, J[2])$ and compute their images in $(K^*/(K^*)^2)^4$.

- Step 3: Follow Section 4.2.2 and compute the morphism $J_\epsilon \subset \mathbb{P}^{15}_{\{u_i,v_i\}} \xrightarrow{proj} \mathbb{P}^9_{u_i} \xrightarrow{(\tilde{\psi_\epsilon})^{-1}\tilde{\phi_\epsilon}} \mathbb{P}^9_{k'_{ij}} \xrightarrow{g_2} \mathcal{K}_\epsilon \subset \mathbb{P}^3_{k'_i}$ in (4.2.1). We showed that k'_{11}, treated as a function on J_ϵ (via the pull back), gives the denominator of f_P, f_Q, f_R, f_S in the formula for $\langle \epsilon, \eta \rangle_{CT}$ in Theorem 4.1.4.

- Step 4: Follow Remark 4.2.6 and find $P_1 \in J$ such that $2P_1 = P$. Then compute the linear map Ψ in Proposition 4.2.5.

- Step 5: Follow Section 4.2.3 with $T = P$, and compute the morphism $J_\epsilon \subset \mathbb{P}^{15}_{\{u_i,v_i\}} \xrightarrow{\phi_\epsilon} J \subset \mathbb{P}^{15}_{\{k_{ij},b_i\}} \xrightarrow{\Psi} \mathbb{P}^9_{kij} \xrightarrow{(\bar{\psi}_{\epsilon+\delta(P)})^{-1}} \mathbb{P}^9_{k'_{ij},P} \xrightarrow{g_2} \mathcal{K}_{\epsilon+\delta(P)} \subset \mathbb{P}^3_{k'_i,P}$ in (4.2.2) using the linear map Ψ computed in Step 4. We showed that $k'_{11,P}$, treated as a function on J_ϵ (via the pull back), gives the numerator of f_P.

- Step 6: Compute $f_P = k'_{11,P}/k'_{11}$, which is a K-rational function on J_ϵ satisfying Remark 4.1.3.

- Step 7: Repeat Steps 4, 5 and 6 with the other generators Q, R, S of $J[2]$ and compute f_Q, f_R, f_S similarly.

- Step 8: Follow Remarks 4.4.6, 4.4.7 and compute the bound $N_{\epsilon,\eta} \in \mathbb{N}$ such that any finite place v of K above any prime bigger than $N_{\epsilon,\eta}$, the local Cassels-Tate pairing between ϵ and η using the formula in Theorem 4.1.4 is trivial.

- Step 9: For any place v of K that is above a prime that is not greater than the number $N_{\epsilon,\eta}$ computed in Step 8, find a local point P_v on J_ϵ avoiding the zeros and poles of f_P, f_Q, f_R, f_S.

- Step 10: Compute $\langle \epsilon, \eta \rangle_{CT}$ via the formula in Theorem 4.1.4.

Using the above algorithm, we can compute the Cassels-Tate pairing matrix for $\text{Sel}^2(J)$, that is a square matrix where the ij^{th} entry represents the Cassels-Tate pairing between the i^{th} and the j^{th} generators of $\text{Sel}^2(J)$. Recall that here we assume all points in $J[2]$ are defined over K, the Cassels-Tate pairing in this case is in fact alternating by Lemma 1.8.3, which simplifies our computation.

Remark 4.5.1. One method for finding a local point P_v on J_ϵ avoiding the zeros and poles of f_P, f_Q, f_R, f_S is by looking for a corresponding local point on $\mathcal{K}_\epsilon \subset \mathbb{P}^3$. Recall that the numerators and denominators of f_P, f_Q, f_R, f_S are linear forms. A linear form on J_ϵ is of the form $f_{even} + f_{odd}$ where f_{even} is linear in the even coordinates and f_{odd} is linear in the odd coordinates. By the explicit defining equations of J_ϵ as discussed in Section 1.11, we know $(f_{even} + f_{odd})(f_{even} - f_{odd})$ is a homogeneous polynomial of degree 4 in the coordinates on $\mathcal{K}_\epsilon$. Hence, it suffices to find a local point on $\mathcal{K}_\epsilon$ that comes from J_ϵ and does not vanish on these corresponding homogeneous polynomials of degree

4. To test if a local point on $\mathcal{K}_\epsilon$ comes from J_ϵ or not, we can compute its corresponding image $(u_0, ...u_9) \in \mathbb{P}^9$ then follow the discussion at the end of Section 1.11. It is more convenient to find local points via this way because $\mathcal{K}_\epsilon \subset \mathbb{P}^3$ is defined by one equation whereas $J_\epsilon \subset \mathbb{P}^{15}$ is defined by a system of 72 equations.

4.5.2 Worked example

Now we follow the steps in Section 4.5.1 with an example. In particular, we will see with this example, that computing the Cassels-Tate pairing on $\text{Sel}^2(J)$ does improve the rank bound obtained via a 2-descent. This genus two curve was kindly provided by my supervisor, Tom Fisher, along with a list of other genus two curves for me to test the algorithm.

Consider the following genus two curve

$$\mathcal{C} : y^2 = -10x(x+10)(x+5)(x-10)(x-5)(x-1).$$

Its Jacobian variety J has all the two-torsion points defined over $\mathbb{Q}$ by Remark 1.2.1. A set of generators of $J[2]$ satisfying the Weil pairing matrix (4.1.1) are

$$P = \{(0,0),(-10,0)\},\ Q = \{(0,0),(-5,0)\},$$
$$R = \{(10,0),(5,0)\},\quad S = \{(10,0),(1,0)\}.$$

- Consider $\epsilon, \eta \in \text{Sel}^2(J)$ represented by $(-33,1,-1,-11)$ and $(11,1,-1,-11)$ respectively, under the isomorphism $H^1(G_\mathbb{Q}, J[2]) \to (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^4$.

- Under the isomorphism $H^1(G_\mathbb{Q}), J[2]) \to (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^4$, the images of $[P], [Q]$, $[R], [S]$ via $\delta : J(\mathbb{Q})/2J(\mathbb{Q}) \to H^1(G_\mathbb{Q}, J[2])$, computed via the formula for the Cassels map, are

$$\delta([P]) = (-66,1,6,22),\ \delta([Q]) = (-1,1,3,1),$$
$$\delta([R]) = (6,3,1,3),\qquad \delta([S]) = (22,1,-3,-11).$$

- Using the coordinates $c_0, ..., c_9, d_1, ..., d_6$ for $J_\epsilon \in \mathbb{P}^{15}$ described below in Remark 4.5.2(i), we have

$$\begin{aligned} k'_{11} &= 618874080c_0 - 496218440c_1 - 390547052c_3 + 205551080c_4 \\ &\quad + 384569291c_6 + 52868640c_8; \end{aligned}$$

$$\begin{aligned} k'_{11,P} &= -36051078800000c_2 + 8111492730000c_3 + 265237150000c_7 \\ &\quad - 196928587500c_8 - 6786529337500c_9 + 22531924250d_2 \\ &\quad - 126449158891d_4 - 117221870375d_5 + 937774963000d_6; \end{aligned}$$

$$k'_{11,Q} = 134800c_1 + 235600c_3 + 62000c_4 + 52235c_6 + 60016d_1 - 5456d_5;$$

$$k'_{11,R} = -30223125c_6 + 4050000c_8 - 49750d_3 + 709236d_4$$

$$\begin{aligned} k'_{11,S} &= 4724524800c_1 + 8557722360c_3 + 13102732800c_4 + 1258642935c_6 \\ &\quad + 7291944000c_9 - 2709362304d_1 + 97246845d_2 + 8475710d_3 \\ &\quad + 30788208d_5. \end{aligned}$$

  Hence, we have explicit formulae for

$$f_P = \frac{k'_{11,P}}{k'_{11}}, f_Q = \frac{k'_{11,Q}}{k'_{11}}, f_R = \frac{k'_{11,R}}{k'_{11}}, f_S = \frac{k'_{11,S}}{k'_{11}}.$$

  In particular, they are defined over $\mathbb{Q}$ as claimed.

- Following Remarks 4.4.6 and 4.4.7, we have the following primes that potentially contribute to $\langle \epsilon, \eta \rangle_{CT}$.
  - Prime 2;
  - Primes of bad reduction of the genus two curve $\mathcal{C}$: $2, 3, 5, 11$;
  - Primes arise from M_ϵ, denoted by S' in Remark 4.4.7(ii): $2, 3, 5, 11, 17, 19, 31, 197, 199$;
  - Primes below 500.

  It turns out that the only nontrivial local Cassels-Tate pairings between ϵ and η are at places $11, 19, \infty$ and $\langle \epsilon, \eta \rangle_{CT} = -1$.

Remark 4.5.2.

(i) In the case where all points of $J[2]$ are defined over the base field, the coordinates in [FTvL12, Definitions 6.9, 6.11] as described in Remark 1.11.2 are Galois invariant and denoted by $c_0, ..., c_9, d_1, ..., d_6$ where $c_0, ..., c_9$ are

even and $d_1, ..., d_6$ are odd. In the above worked example, we embedded $J_\epsilon \subset \mathbb{P}^{15}$ with this set of coordinates instead of the coordinates $u_0, ..., u_9, v_1, ..., v_6$ given in Theorem 1.11.1.

(ii) As discussed in Remark 4.4.7, we probably have computed the local Cassels-Tate pairing for more primes than needed. We also suspect that via some suitable minimization and reduction techniques, we can simplify the set of primes that potentially contribute to $\langle \epsilon, \eta \rangle_{CT}$. However, this does not have much effect on the computation as the local Cassels-Tate paring is fast to compute, even for very large primes.

(iii) We list a few sanity checks throughout the computation. We verified that all the defining equations of the twisted Kummer surfaces are indeed defined over $\mathbb{Q}$. For each local Cassels-Tate pairing computations, we computed 100 local points at random and verified that these local points all give the same value of the local pairing.

Under the isomorphism $H^1(G_\mathbb{Q}, J[2]) \to (\mathbb{Q}^*/(\mathbb{Q}^*)^2)^4$, $\mathrm{Sel}^2(J)$ has size 2^6 and is generated by

$$(-33, 1, -1, -11), (11, 1, -1, -11), (66, 1, 2, 22),$$
$$(11, 1, 2, 22), (3, 3, 3, 3), (3, 1, 3, 1).$$

Since $\mathcal{C}$ has rational points, we know the Cassels-Tate pairing is alternating by Lemma 1.8.3. Since all the two-torsion points on J are rational and $\langle \epsilon, \eta \rangle_{CT} = -1$, we get $|\ker\langle\ ,\ \rangle_{CT}| = 2^4$.

Indeed, we verified that the Cassels-Tate pairing matrix, with the generators of $\mathrm{Sel}^2(J)$ listed above, is

$$\begin{bmatrix} 1 & -1 & 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 1 & -1 & -1 & 1 \end{bmatrix},$$

which is a rank 2 matrix.

Recall in Remark 1.9.4(i), we showed that we can potentially improve the rank bound from the standard descent calculation via computing the Cassels-Tate pairing as $J(\mathbb{Q})/2J(\mathbb{Q}) \subset \ker\langle\ ,\ \rangle_{CT} \subset \mathrm{Sel}^2(J)$. This is indeed true and in this example, we improve the rank bound from $2^r \leq |\mathrm{Sel}^2(J)|/|J(\mathbb{Q})[2]| = 2^2$ to $2^r \leq |\ker\langle\ ,\ \rangle_{CT}|/|J(\mathbb{Q})[2]| = 2^0$. Therefore, we not only improved the rank bound but also proved that the rank of this particular Jacobian variety is in

fact equal to 0.

Also recall in Proposition 1.9.3 and Remark 1.9.4(ii), we proved that in the case where all points in $J[2]$ are defined over the base field, computing the Cassels-Tate pairing on $\mathrm{Sel}^2(J)$ gives the same rank bound as obtained from carrying out a $4-$descent which involves computing $\mathrm{Sel}^4(J)$. More specifically, we have $\mathrm{Im}\,\alpha = \ker\langle\ ,\ \rangle_{CT}$, where α is defined in the following exact sequence :

$$0 \to J[2](K) \to J[4](K) \to J[2](K) \to \mathrm{Sel}^2(J) \to \mathrm{Sel}^4(J) \xrightarrow{\alpha} \mathrm{Sel}^2(J).$$

Chapter 5

The Cassels-Tate Pairing with Points on the Twisted Kummer

In this chapter, we let J denote the Jacobian variety of a genus two curve $\mathcal{C}$ that is defined by $y^2 = f(x) = f_6x^6 + ... + f_0$ such that f is a degree 6 polynomial defined over the base field K. For $\epsilon, \eta \in \text{Sel}^2(J)$, we will prove an explicit formula for the Cassels-Tate pairing $\langle \epsilon, \eta \rangle_{CT}$ under the assumption that the twisted Kummer surface $\mathcal{K}_\eta$ defined in Remark 1.6.3 has a K-rational point. In this chapter, the field K is a number field, unless stated otherwise. We will then describe an algorithm that explicitly computes the pairing using this formula. This algorithm becomes more practical in the case where $K = \mathbb{Q}$ and the size of the Galois group of f is relatively small. In Chapter 6, we will give a modified algorithm for computing the pairing using this formula which works in the general case.

5.1 Formula for the Cassels-Tate pairing

In this section, we state and prove an explicit formula for $\langle \epsilon, \eta \rangle_{CT}$ with $\epsilon, \eta \in \text{Sel}^2(J)$ under the assumption that the twisted Kummer surface $\mathcal{K}_\eta$ has a K-rational point.

5.1.1 Statement of the formula

Consider $\epsilon \in \text{Sel}^2(J)$. Let $(J_\epsilon, \pi_\epsilon)$ be the 2-covering of J corresponding to ϵ. There exists an isomorphism ϕ_ϵ defined over $\bar{K}$ such that $[2] \circ \phi_\epsilon = \pi_\epsilon$ which is defined over K and a linear isomorphism $\psi_\epsilon : \mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ defined over $\bar{K}$ satisfying the usual commutative diagram (1.6.2).

Suppose R is a K-rational point on the twisted Kummer $\mathcal{K}_\epsilon$. Let Q_1, Q_2 denote the two preimages of R via the degree two morphism $J_\epsilon \xrightarrow{|\phi_\epsilon^*(2\Theta)|} \mathcal{K}_\epsilon \subset \mathbb{P}^3$. From the discussion at the end of Section 1.11, we know there exists a nonzero $a \in K$ such that $K(Q_1) = K(Q_2) = K(\sqrt{a})$. Moreover, a is explicitly computable given the defining equation of $\mathcal{C}$, ϵ and the coordinates of R. Then, by Corollary 1.5.6, we know J_ϵ is a trivial principal homogeneous space of J

considered as a variety defined over $K(\sqrt{a})$.

Now we state the following theorem on the formula for the Cassels-Tate pairing.

Theorem 5.1.1. *Let J be the Jacobian variety of a genus two curve $\mathcal{C}$ defined over a number field K. For $\epsilon, \eta \in Sel^2(J)$, let $(J_\epsilon, \pi_\epsilon), (J_\eta, \pi_\eta)$ denote the corresponding 2-coverings of J. Suppose $\mathcal{K}_\eta$, the twisted Kummer surface corresponding to η, has a K-rational point R and the field of definition of the preimages of R on J_η is $K(\sqrt{a})$ for some nonzero $a \in K$. Then there exists a K-rational function g on J_ϵ, which also depends on η, such that*

$$\langle \epsilon, \eta \rangle_{CT} = \prod_{place\ v} (g(P_v), a)_v,$$

where $(\ ,\ )_v$ denotes the Hilbert symbol for a given place v of K and P_v is an arbitrary choice of a local point on J_ϵ avoiding the zeros and poles of g.

Remark 5.1.2. Similar to Remark 4.1.5, we will show that the formula for the Cassels-Tate pairing given in Theorem 5.1.1 is in fact always a finite product.

5.1.2 Proof of the formula

In this section, we give a proof for Theorem 5.1.1. Suppose the twisted Kummer $\mathcal{K}_\eta$ for $\eta \in \mathrm{Sel}^2(J)$ has a K-rational point. We have the following lemmas computing a cocycle representation of the image of η in $H^1(G_K, J)$.

Lemma 5.1.3. *Let (J_η, π_η) be the 2-covering of J that corresponds to $\eta \in H^1(G_K, J[2])$. Let $\phi_\eta : J_\eta \to J$ be an isomorphism defined over $\bar{K}$ with $\pi_\eta = [2] \circ \phi_\eta$. Then, for any $Q \in J_\eta$, the image of η in $H^1(G_K, J)$ is represented by the cocycle $\sigma \mapsto \phi_\eta(Q) - \phi_\eta(\sigma(Q))$.*

Proof. We know $\eta \in H^1(G_K, J[2])$ is represented by the cocycle $\sigma \mapsto \eta_\sigma$ where $\phi_\eta(\phi_\eta^{-1})^\sigma$ is translation by η_σ. Therefore $\eta_\sigma = \phi_\eta(\sigma(Q)) - \sigma(\phi_\eta(Q))$. This differs from the cocycle in the statement of the lemma by the coboundary $\sigma \mapsto \sigma(\phi_\eta(Q)) - \phi_\eta(Q)$.

□

Lemma 5.1.4. *Let (J_η, π_η) be the 2-covering of J that corresponds to $\eta \in H^1(G_K, J[2])$. Let R be a K-rational point on the twisted Kummer $\mathcal{K}_\eta$ with the field of definition of its preimages Q_1, Q_2 on J_η being $K(\sqrt{a})$ for some nonzero $a \in K$. Let $S = \pi_\eta(Q_1)$. Then the image of η in $H^1(G_K, J)$ is represented by the cocycle*

$$\sigma \mapsto \begin{cases} \mathcal{O}_J & \text{if } \sigma(\sqrt{a}) = \sqrt{a}, \\ S & \text{if } \sigma(\sqrt{a}) = -\sqrt{a}. \end{cases}$$

Proof. Let $\phi_\eta : J_\eta \to J$ be an isomorphism defined over $\bar{K}$ with $\pi_\eta = [2]\circ\phi_\eta$. By Notation 1.6.4, the involution ι_η on J_η such that $[-1]\circ\phi_\eta = \phi_\eta\circ\iota_\eta$ is defined over K and swaps over Q_1 and Q_2. In particular, $\phi_\eta(Q_2) = \phi_\eta(\iota_\eta(Q_1)) = -\phi_\eta(Q_1)$.

We take $Q = Q_1$ in Lemma 5.1.3. If $\sigma(\sqrt{a}) = \sqrt{a}$, then $\phi_\eta(Q_1) - \phi_\eta(\sigma(Q_1)) = \phi_\eta(Q_1) - \phi_\eta(Q_1) = \mathcal{O}_J$. If $\sigma(\sqrt{a}) = -\sqrt{a}$, then $\phi_\eta(Q_1) - \phi_\eta(\sigma(Q_1)) = \phi_\eta(Q_1) - \phi_\eta(Q_2) = 2\phi_\eta(Q_1) = \pi_\eta(Q_1) = S$.

□

Remark 5.1.5. Follow the notation and condition in Lemma 5.1.4. If a is a square in K, then J_η has a K-rational point which makes it a trivial torsor by Corollary 1.5.6 and the cocycle given in the above lemma is indeed trivial. Suppose a is not a square in K and $G_{K(\sqrt{a})/K} = \{1, \sigma\}$. The lemma above shows that the image of η is the image via the inflation map of the element in $H^1(G_{K(\sqrt{a})/K}, J(K(\sqrt{a})))$ represented by the cocycle

$$(1 \mapsto \mathcal{O}_J, \sigma \mapsto S).$$

We now define the twisted group law in the lemma below.

Lemma 5.1.6. *Let $(J_\epsilon, \pi_\epsilon), (J_\eta, \pi_\eta)$ and $(J_{\epsilon+\eta}, \pi_{\epsilon+\eta})$ be the 2-coverings of J corresponding to ϵ, η and $\epsilon+\eta$ in $H^1(G_K, J[2])$. Let $\phi_\epsilon : J_\epsilon \to J$ and $\phi_\eta : J_\eta \to J$ be isomorphisms defined over $\bar{K}$ satisfying $\pi_\epsilon = [2]\circ\phi_\epsilon$ and $\pi_\eta = [2]\circ\phi_\eta$. If we make a suitable choice of $\phi_{\epsilon+\eta}$, an isomorphism $J_{\epsilon+\eta} \to J$ defined over $\bar{K}$ satisfying $\pi_{\epsilon+\eta} = [2]\circ\phi_{\epsilon+\eta}$, then there exists a morphism μ defined over K making the following diagram commute*

$$\begin{array}{ccccc} J_\epsilon & \times & J_\eta & \xrightarrow{\mu} & J_{\epsilon+\eta} \\ \downarrow{\scriptstyle \phi_\epsilon} & & \downarrow{\scriptstyle \phi_\eta} & & \downarrow{\scriptstyle \phi_{\epsilon+\eta}} \\ J & \times & J & \xrightarrow{+} & J \end{array} .$$

Proof. We know the cocycle $(\sigma \mapsto \epsilon_\sigma)$ represents ϵ, where $\phi_\epsilon(\phi_\epsilon^{-1})^\sigma$ is the translation by $\epsilon_\sigma \in J$ and we have similar results for η_σ. By Remark 1.5.4(ii), we can always find an isomorphism $\phi_{\epsilon+\eta} : J_{\epsilon+\eta} \to J$, with the cocycle condition that $\epsilon_\sigma + \eta_\sigma = (\epsilon+\eta)_\sigma$.

Let $\mu : J_\epsilon \times J_\eta \to J_{\epsilon+\eta}$ be the morphism that makes the diagram in the lemma commute. For any $P, Q \in J$ and any $\sigma \in G_K$, we then have the following

$$\begin{aligned}\mu^{\sigma}(\phi_{\epsilon}^{-1}(P),\phi_{\eta}^{-1}(Q)) &= \sigma(\mu(\phi_{\epsilon}^{-1}(\phi_{\epsilon}(\phi_{\epsilon}^{-1})^{(\sigma^{-1})}(P^{(\sigma^{-1})})),\phi_{\eta}^{-1}(\phi_{\eta}(\phi_{\eta}^{-1})^{(\sigma^{-1})}(Q^{(\sigma^{-1})}))))\\ &= \sigma(\phi_{\epsilon+\eta}^{-1}(P^{(\sigma^{-1})}+Q^{(\sigma^{-1})}+\epsilon_{\sigma^{-1}}+\eta_{\sigma^{-1}}))\\ &= \phi_{\epsilon+\eta}^{-1}(P+Q)\\ &= \mu(\phi_{\epsilon}^{-1}(P),\phi_{\eta}^{-1}(Q)).\end{aligned}$$

Hence, μ is indeed defined over K.

□

Corollary 5.1.7. *Let $(J_\epsilon,[2]\circ\phi_\epsilon),(J_\eta,[2]\circ\phi_\eta)$ and $(J_{\epsilon+\eta},[2]\circ\phi_{\epsilon+\eta})$ be the 2-coverings of J corresponding to ϵ, η and $\epsilon+\eta$ in $Sel^2(J)$ that satisfy the condition in Lemma 5.1.6. Suppose the twisted Kummer surface $\mathcal{K}_\eta$ has a K-rational point R. Let $Q\in J_\eta$ be a preimage of R and $K(Q)=K(\sqrt{a})$. Let $P=\phi_\eta(Q)\in J$. Consider the isomorphism $\phi: J_\epsilon\to J_{\epsilon+\eta}$ that makes the following diagram commute:*

$$\begin{array}{ccc} J_\epsilon & \xrightarrow{\phi} & J_{\epsilon+\eta} \\ \downarrow{\scriptstyle \phi_\epsilon} & & \downarrow{\scriptstyle \phi_{\epsilon+\eta}} \\ J & \xrightarrow{\tau_P} & J. \end{array}$$

We have ϕ is defined over $K(\sqrt{a})$.

Proof. By Lemma 5.1.6, we have a morphism $\mu: J_\epsilon\times J_\eta\to J_{\epsilon+\eta}$ defined over K and $\phi=\mu(-,Q)$. This implies that ϕ is defined over $K(Q)=K(\sqrt{a})$.

□

Now we will give a proof for Theorem 5.1.1 using the lemmas proved above.

Proof of Theorem 5.1.1. We will show that the formula given in the theorem is indeed the Cassels-Tate pairing following the homogeneous space definition as defined in Section 1.8.2.

First, we notice that if the preimages of R are in fact defined over K and a is a nonzero square in K, then J_η has a K-rational point. By Corollary 1.5.6, we know that J_η is the trivial homogeneous space and the image of η in $H^1(G_K,J)$ is the trivial element. By the bilinearity of the Cassels-Tate pairing, we know that $\langle\epsilon,\eta\rangle_{CT}$ is trivial. On the other hand, since a is a nonzero square in K, then the Hilbert symbol between a and anything else is 1 by definition. Hence, we can take g to be any K-rational function on J_ϵ, for example the constant function on J_ϵ that always takes the value 1.

Now we assume a is not a square in K. Let $\phi_\epsilon : J_\epsilon \to J, \phi_\eta : J_\eta \to J$ be two isomorphisms such that $[2] \circ \phi_\epsilon = \pi_\epsilon$ and $[2] \circ \phi_\eta = \pi_\eta$. Then, there exists an isomorphism $\phi_{\epsilon+\eta} : J_{\epsilon+\eta} \to J$ such that $(J_{\epsilon+\eta}, [2] \circ \phi_{\epsilon+\eta})$ is the 2-covering of J corresponding to $\epsilon + \eta$ and the condition in Lemma 5.1.6 is satisfied.

Let $Q \in J_\eta(K(\sqrt{a}))$ be a preimage of R and $P = \phi_\eta(Q) \in J$. By Lemma 5.1.4, we know that the image of η in $H^1(G_K, J)$ is represented by the following cocycle

$$\sigma \mapsto \begin{cases} \mathcal{O}_J & \text{if } \sigma(\sqrt{a}) = \sqrt{a}, \\ 2P & \text{if } \sigma(\sqrt{a}) = -\sqrt{a}. \end{cases}$$

Following the homogeneous space definition of $\langle \epsilon, \eta \rangle_{CT}$, we have the corresponding element in $H^1(G_K, \mathrm{Pic}^0(J))$ represented by the following cocycle

$$\sigma \mapsto \begin{cases} \mathrm{id} & \text{if } \sigma(\sqrt{a}) = \sqrt{a}, \\ [\tau_{2P}^* \Theta - \Theta] & \text{if } \sigma(\sqrt{a}) = -\sqrt{a}. \end{cases}$$

Recall we have the isomorphism $\phi = \phi_{\epsilon+\eta}^{-1} \tau_P \phi_\epsilon$ defined over $K(\sqrt{a})$ in Corollary 5.1.7. Then, let H_ϵ on J_ϵ be the pull back of any fixed hyperplane section on $\mathcal{K}_\epsilon$ via $J_\epsilon \xrightarrow{|\phi_\epsilon^*(2\Theta)|} \mathcal{K}_\epsilon$ and $H_{\epsilon+\eta}$ on $J_{\epsilon+\eta}$ be the pull back of any fixed hyperplane section on $\mathcal{K}_{\epsilon+\eta}$ via $J_{\epsilon+\eta} \xrightarrow{|\phi_{\epsilon+\eta}^*(2\Theta)|} \mathcal{K}_{\epsilon+\eta}$. Define $\Xi = \phi^* H_{\epsilon+\eta} - H_\epsilon$. We have

$$\begin{aligned} (\phi_\epsilon^{-1})^*(\Xi) &= (\phi_\epsilon^{-1})^*(\phi^* H_{\epsilon+\eta} - H_\epsilon) \\ &\sim (\phi_\epsilon^{-1})^*((\phi_{\epsilon+\eta}^{-1} \tau_P \phi_\epsilon)^*(\phi_{\epsilon+\eta}^*(2\Theta)) - \phi_\epsilon^*(2\Theta)) \\ &= \tau_P^*(2\Theta) - 2\Theta. \end{aligned}$$

Since $\tau_P^*(2\Theta) - 2\Theta \sim \tau_{2P}^*\Theta - \Theta$, the corresponding element in $H^1(G_K, \mathrm{Pic}^0(J_\epsilon))$ is represented by the cocycle

$$\sigma \mapsto \begin{cases} \mathrm{id} & \text{if } \sigma(\sqrt{a}) = \sqrt{a}, \\ [\Xi] & \text{if } \sigma(\sqrt{a}) = -\sqrt{a}. \end{cases}$$

Then we consider the image of the following cochain in $C^1(G_K, \mathrm{Div}^0(J))$ under the homomorphism $d : C^1(G_K, \mathrm{Div}^0(J)) \to C^2(G_K, \mathrm{Div}^0(J))$, described in Section 1.4.

$$\sigma \mapsto \begin{cases} \mathrm{id} & \text{if } \sigma(\sqrt{a}) = \sqrt{a}, \\ \Xi & \text{if } \sigma(\sqrt{a}) = -\sqrt{a}. \end{cases}$$

Since ϕ is defined over $K(\sqrt{a})$ and Ξ is defined over $K(\sqrt{a})$, we compute that the image of the above cochain under the homomorphism d is

$$(\sigma_1, \sigma_2) \mapsto \begin{cases} \phi^* H_{\epsilon+\eta} + \sigma_1(\phi^* H_{\epsilon+\eta}) - 2H_\epsilon & \text{if } \sigma_1(\sqrt{a}) = \sigma_2(\sqrt{a}) = -\sqrt{a}, \\ \mathrm{id} & \text{otherwise.} \end{cases}$$

Let $G_{K(\sqrt{a})/K} = \{1, \sigma\}$. Since ϕ is defined over $K(\sqrt{a})$, we have $\sigma(\phi^* H_{\epsilon+\eta}) = \sigma_1(\phi^* H_{\epsilon+\eta})$ for any $\sigma_1 \in G_K$ such that $\sigma_1(\sqrt{a}) = -\sqrt{a}$. Following the homogeneous space definition of the Cassels-Tate pairing, there exists a K-rational function g on J_ϵ such that

$$\mathrm{div}(g) = \phi^* H_{\epsilon+\eta} + \sigma(\phi^* H_{\epsilon+\eta}) - 2H_\epsilon.$$

And for each place v of K, we need to consider the element c_v in $H^2(G_{K_v}, \bar{K_v}^*)$ represented by the cocycle

$$(\sigma_1, \sigma_2) \mapsto \begin{cases} g(P_v) & \text{if } \sigma_1(\sqrt{a}) = \sigma_2(\sqrt{a}) = -\sqrt{a}, \\ 1 & \text{otherwise,} \end{cases}$$

where P_v is any local point on J_ϵ avoiding the zeros and poles of g.

By Lemma 4.1.6, we know that the element $c_v \in H^2(G_{K_v}, \bar{K_v}^*) \cong \mathrm{Br}(K_v)$ is the class of the quaternion algebra $(g(P_v), a)$. Moreover, by Lemma 1.4.19, we know $\mathrm{inv}((g(P_v), a)) = (g(P_v), a)_v$ as required.

□

Remark 5.1.8. Follow the condition and notation in Theorem 5.1.1. We know $\langle \epsilon, \eta \rangle_{CT}$ is trivial if $K(\sqrt{a}) = K$. Now suppose $G_{K(\sqrt{a})/K} = \{1, \sigma\}$. From the proof of Theorem 5.1.1, the K-rational function g in the statement of Theorem 5.1.1 has divisor of zeros and poles precisely at $\phi^* H_{\epsilon+\eta} + \sigma(\phi^* H_{\epsilon+\eta}) - 2H_\epsilon$, where H_ϵ on J_ϵ is the pull back of any fixed hyperplane section on $\mathcal{K}_\epsilon$ and $H_{\epsilon+\eta}$ on $J_{\epsilon+\eta}$ is the pull back of any fixed hyperplane section on $\mathcal{K}_{\epsilon+\eta}$. To explicitly compute $\langle \epsilon, \eta \rangle_{CT}$, we need to explicitly compute such g which is done in the next section.

5.2 Explicit Computation

In this section, we give a method for explicitly computing the formula for the Cassels-Tate pairing of $\epsilon, \eta \in \mathrm{Sel}^2(J)$, as stated in Theorem 5.1.1 and explained in Remark 5.1.8. For $T \in J$, we let $k(T) = (k_1(T), k_2(T), k_3(T), k_4(T))$, where $k_1, ..., k_4$ is the basis for $\mathcal{L}(\Theta^+ + \Theta^-)$ and the fixed coordinates on $\mathcal{K} \subset \mathbb{P}^3$ as described in Section 1.3.2.

5.2.1 $(2, 2, 2)$-form

In this section, we introduce a $(2, 2, 2)$-form $\mathcal{F}$. This will be shown to be related to the explicit computation for the function g that appears in the formula for the Cassels-Tate pairing in Theorem 5.1.1.

Recall the genus two curve is defined by $y^2 = f(x) = f_6 x^6 + ... + f_0$. In Corollary 1.3.7, we showed that, for $S, T \in J$ and $i, j \in \{1, ..., 4\}$, there exist

symmetric biquadratic forms ψ_{ij} defined over $\mathbb{Z}[f_0, ..., f_6]$ with explicit formulae, such that the 4 by 4 matrix $(\psi_{ij}(k(S), k(T)))$ is projectively equal to

$$k_i(S-T)k_j(S+T) + k_j(S-T)k_i(S+T).$$

We define $\lambda(S,T)$, independent of i and j, such that

$$\psi_{ij}(k(S), k(T))) = \lambda(S,T)\big(k_i(S-T)k_j(S+T) + k_j(S-T)k_i(S+T)\big).$$

Since $k_1 = 1$, we get that $\lambda(S,T) = \frac{\psi_{11}(k(S),k(T))}{2}$. By the explicit formula for ψ_{11}, we verify that $S \mapsto \lambda(S,T)$ is never the zero function on J for any $T \in J$. The lemma below constructs a $(2,2,2)$-form.

Lemma 5.2.1. *Let $x = (x_1, x_2, x_3, x_4), y = (y_1, y_2, y_3, y_4), z = (z_1, z_2, z_3, z_4)$ be three vectors. Then*

$$\mathcal{F}(x,y,z) = \sum_{i=1}^{4}\sum_{j=1}^{4} z_i \psi_{ij}(x,y) z_j$$

is a $(2,2,2)$-form that is defined over K, symmetric in the first two sets of coordinates and it vanishes on $(k(S), k(T), c)$, for any $S, T \in J$ and column vector $c = (c_1, c_2, c_3, c_4)$ such that $c^T k(S+T) = 0$.

Proof. Since $\sum_{i=1}^{4} k_i(S+T)c_i = 0$, we get

$$\begin{aligned}
&\sum_{i=1}^{4}\sum_{j=1}^{4} c_i \psi_{ij}(k(S), k(T)) c_j \\
=&\lambda(S,T)\sum_{i=1}^{4}\sum_{j=1}^{4} c_i\big(k_j(S+T)k_i(S-T) + k_i(S+T)k_j(S-T)\big)c_j \\
=&0.
\end{aligned}$$

Also, the $(2,2,2)$-form $\mathcal{F}$ is defined over K and symmetric in the first two sets of coordinates as each ψ_{ij} is defined over K and symmetric.

□

We also state and prove the following two lemmas that describe some properties of $\mathcal{F}$.

Lemma 5.2.2. *Fix any $T \in J$ and $c = (c_1, c_2, c_3, c_4)$ not a zero vector. For $S \in J$,*

$$S \mapsto \mathcal{F}(k(S), k(T), c)$$

is not the zero function on J.

Proof. By the definition of $\mathcal{F}$,

$$\mathcal{F}(k(S),k(T),c)=\sum_{i=1}^{4}\sum_{j=1}^{4}c_i\psi_{ij}(k(S),k(T))c_j,$$

which is equal to

$$\begin{aligned}&\lambda(S,T)\sum_{i=1}^{4}\sum_{j=1}^{4}c_i\big(k_i(S-T)k_j(S+T)+k_j(S-T)k_i(S+T)\big)c_j\\ =&2\lambda(S,T)\cdot\big(\sum_{i=1}^{4}c_ik_i(S-T)\big)\cdot\big(\sum_{j=1}^{4}k_j(S+T)c_j\big).\end{aligned}$$

Moreover, we know $S\mapsto\lambda(S,T)$ is not the zero function on J. Recall $k_1,...,k_4$ form a basis for $\mathcal{L}(\Theta^+ + \Theta^-)$. We note that $\{(S\mapsto k_i(S-T)), i=1,...,4\}$ form a basis for $\mathcal{L}(\tau_{-T}^*(\Theta^+ + \Theta^-))$ and $\{(S\mapsto k_j(S+T)), i=1,...,4\}$ form a basis for $\mathcal{L}(\tau_T^*(\Theta^+ + \Theta^-))$. Since c_i are not all zero, both $S\mapsto\sum_{i=1}^4 c_ik_i(S-T)$ and $S\mapsto\sum_{j=1}^4 k_j(S+T)c_j$ are not the zero function on J. Hence, $S\mapsto\mathcal{F}(k(S),k(T),c)$ is not the zero function on J as required.

□

Lemma 5.2.3. *Suppose $T_1,T_2,T_3\in J[2]$ satisfy $T_1+T_2+T_3=O_J$. Let $M_{T_1},M_{T_2},M_{T_3}\in GL_4(\bar{K})$ represent the action of translations by T_1,T_2,T_3 on $\mathcal{K}\subset\mathbb{P}^3$, respectively. Then*

$$\mathcal{F}(M_{T_1}x,M_{T_2}y,M_{T_3}^Tz)=\kappa\mathcal{F}(x,y,z)$$

as polynomials in x,y,z for some constant $\kappa\in\bar{K}$.

Proof. We decided to prove it by a generic calculation. Suppose the defining polynomial of the genus two curve is $y^2=f(x)=\lambda(x-\omega_1)(x-\omega_2)\cdots(x-\omega_6)$. Let $K'=\mathbb{Q}(\lambda,\omega_1,...,\omega_6)$ and then the coefficients of f are defined over K'. Recall for $T=\{(\omega_i,0),(\omega_j,0)\}$ we have formulae for M_T defined over K' in [CF96, Chapter 3, Section 2]. Also by Lemma 5.2.1, we know that the coefficients of $\mathcal{F}$ are defined over $\mathbb{Z}[f_0,...,f_6]$ and so are defined over K'. Hence, it suffices to verify the statement of the lemma over K'. Note by symmetry of the roots, we only need to check 3 cases: $T_1=\{(\omega_1,0),(\omega_2,0)\}$ with $T_2=\{(\omega_1,0),(\omega_3,0)\}$, $T_1=\{(\omega_1,0),(\omega_2,0)\}$ with $T_2=\{(\omega_3,0),(\omega_4,0)\}$, and $T_1=T_2=\{(\omega_1,0),(\omega_2,0)\}$. This reduces the statement to linear algebra over K' and we used MAGMA to verify it.

□

5.2.2 Twisted $(2,2,2)$-form

In this section, we twist the $(2,2,2)$-form $\mathcal{F}$, by $\epsilon, \eta, \epsilon+\eta \in \mathrm{Sel}^2(J)$. More explicitly, let $(J_\epsilon, [2]\circ\phi_\epsilon), (J_\eta, [2]\circ\phi_\eta), (J_{\epsilon+\eta}, [2]\circ\phi_{\epsilon+\eta})$ be the 2-coverings of J corresponding to $\epsilon, \eta, \epsilon+\eta$ that satisfy the condition in Lemma 5.1.6. We let $\theta_\epsilon : J_\epsilon \to \mathcal{K}_\epsilon \subset \mathbb{P}^3$, $\theta_\eta : J_\eta \to \mathcal{K}_\eta \subset \mathbb{P}^3$, $\theta_{\epsilon+\eta} : J_{\epsilon+\eta} \to \mathcal{K}_{\epsilon+\eta} \subset \mathbb{P}^3$ denote the morphisms induced by $|\phi_\epsilon^*(2\Theta)|, |\phi_\eta^*(2\Theta)|, |\phi_{\epsilon+\eta}^*(2\Theta)|$ respectively. Let $\psi_\epsilon, \psi_\eta, \psi_{\epsilon+\eta}$ be the corresponding linear isomorphisms $\mathbb{P}^3 \to \mathbb{P}^3$ that satisfy (1.6.2). Suppose $N_\epsilon, N_\eta, N_{\epsilon+\eta} \in \mathrm{GL}_4(\bar{K})$ represent these linear isomorphisms. We define the corresponding twisted $(2,2,2)$-form $\mathcal{F}_{\epsilon,\eta}(x,y,z)$ as

$$\mathcal{F}(N_\epsilon x, N_\eta y, (N_{\epsilon+\eta}^T)^{-1} z),$$

Note that $\mathcal{F}_{\epsilon,\eta}$ depends on the choice of $N_\epsilon, N_\eta, N_{\epsilon+\eta}$ and is only defined up to scalar multiplication.

Proposition 5.2.4. *There exists a constant $\mu \in \bar{K}$ such that $\frac{1}{\mu}\mathcal{F}_{\epsilon,\eta}(x,y,z)$ is defined over K.*

Proof. We know $\phi_\epsilon(\phi_\epsilon^{-1})^\sigma = \tau_{\epsilon_\sigma}, \phi_\eta(\phi_\eta^{-1})^\sigma = \tau_{\eta_\sigma}$ where $(\sigma \mapsto \epsilon_\sigma), (\sigma \mapsto \eta_\sigma)$ are cocycles representing ϵ, η respectively and $\phi_{\epsilon+\eta}(\phi_{\epsilon+\eta}^{-1})^\sigma$ is the translation by $\epsilon_\sigma + \eta_\sigma$. Let $M_T \in \mathrm{GL}_4(\bar{K})$ represents the action of translation by $T \in J[2]$ on $\mathcal{K} \subset \mathbb{P}^3$. We have $N_\epsilon(N_\epsilon^{-1})^\sigma = M_{\epsilon_\sigma} \in \mathrm{PGL}_4(\bar{K})$, $N_\eta(N_\eta^{-1})^\sigma = M_{\eta_\sigma} \in \mathrm{PGL}_4(\bar{K})$, and $N_{\epsilon+\eta}(N_{\epsilon+\eta}^{-1})^\sigma = M_{\epsilon_\sigma+\eta_\sigma} \in \mathrm{PGL}_4(\bar{K})$. Therefore, for $\sigma \in G_K$, by Lemma 5.2.3 and the fact that $\mathcal{F}$ is defined over K, we have

$$\begin{aligned}
&\mathcal{F}^\sigma_{\epsilon,\eta}(x,y,z)\\
=&\mathcal{F}(N_\epsilon^\sigma x, N_\eta^\sigma y, ((N_{\epsilon+\eta}^T)^{-1})^\sigma z)\\
=&\mathcal{F}(N_\epsilon^\sigma N_\epsilon^{-1} N_\epsilon x, N_\eta^\sigma N_\eta^{-1} N_\eta y, (N_{\epsilon+\eta}(N_{\epsilon+\eta}^{-1})^\sigma)^T (N_{\epsilon+\eta}^T)^{-1} z)\\
=&\lambda_\sigma \mathcal{F}(M_{\epsilon_\sigma} N_\epsilon x, M_{\eta_\sigma} N_\eta y, (M_{\epsilon_\sigma+\eta_\sigma})^T (N_{\epsilon+\eta}^T)^{-1} z)\\
=&\lambda'_\sigma \mathcal{F}(N_\epsilon x, N_\eta y, (N_{\epsilon+\eta}^T)^{-1} z)\\
=&\lambda'_\sigma \mathcal{F}_{\epsilon,\eta}(x,y,z),
\end{aligned}$$

for all $\sigma \in G_K$ with some constants $\lambda_\sigma, \lambda'_\sigma \in \bar{K}$ that only depend on σ.

For any $\sigma_1, \sigma_2 \in G_K$, we have $\lambda'_{\sigma_1\sigma_2} = \sigma_1(\lambda'_{\sigma_2})\lambda'_{\sigma_1}$. Therefore $(\sigma \mapsto \lambda'_\sigma)$ represents a cocycle in $H^1(G_K, \bar{K}^*)$. Since $H^1(G_K, \bar{K}^*)$ is trivial by Hilbert's Theorem 90, we know that there exists $\mu \in \bar{K}$ such that $\lambda'_\sigma = \sigma(\mu)/\mu$ for all $\sigma \in G_K$. Hence, for any $\sigma \in G_K$, we have

$$\sigma(\frac{1}{\mu}\mathcal{F}_{\epsilon,\eta}) = \frac{1}{\mu}\mathcal{F}_{\epsilon,\eta},$$

as required.

□

Remark 5.2.5. By Proposition 5.2.4, we can assume the $(2,2,2)$-form $\mathcal{F}_{\epsilon,\eta}$ is defined over K, for any $\epsilon, \eta \in \mathrm{Sel}^2(J)$. Note that this is still up to scalar multiplication in K. Since we will only need to look at the vanishing of $\mathcal{F}_{\epsilon,\eta}$, this will not be a problem.

Recall that in Lemma 5.1.6 we showed that there exists the twisted group law $\mu : J_\epsilon \times J_\eta \to J_{\epsilon+\eta}$ that is defined over K. We have the following lemma following Lemma 5.2.1 and the definition of $\mathcal{F}_{\epsilon,\eta}$.

Lemma 5.2.6. *For any $P_1 \in J_\epsilon, P_2 \in J_\eta$ and column vector $c = (c_1, c_2, c_3, c_4)$ such that $c^T\theta_{\epsilon+\eta}(\mu(P_1, P_2)) = 0$, we have*

$$\mathcal{F}_{\epsilon,\eta}(\theta_\epsilon(P_1), \theta_\eta(P_2), c) = 0.$$

Proof. By definition of $\mathcal{F}_{\epsilon,\eta}$, it suffices to prove

$$\mathcal{F}(N_\epsilon\theta_\epsilon(P_1), N_\eta\theta_\eta(P_2), (N^T_{\epsilon+\eta})^{-1}c) = \mathcal{F}(k(\phi_\epsilon(P_1)), k(\phi_\eta(P_2)), (N^T_{\epsilon+\eta})^{-1}c) = 0.$$

Since $c^T\theta_{\epsilon+\eta}(\mu(P_1, P_2)) = 0$, we have

$$\begin{aligned} &((N^T_{\epsilon+\eta})^{-1}c)^T k\big(\phi_\epsilon(P_1) + \phi_\eta(P_2)\big) \\ &= c^T N^{-1}_{\epsilon+\eta} k(\phi_{\epsilon+\eta}\mu(P_1, P_2)) \\ &= c^T\theta_{\epsilon+\eta}(\mu(P_1, P_2)) \\ &= 0 \end{aligned}$$

Then we are done by Lemma 5.2.1.

□

5.2.3 Constructing the rational function g

We follow the notation defined at the start of Section 5.2.2. Consider any $P \in J$. Let $\phi : J_\epsilon \to J_{\epsilon+\eta}$ be an isomorphism such that $\phi = \phi^{-1}_{\epsilon+\eta} \circ \tau_P \circ \phi_\epsilon$. Recall we denote the induced involutions on $J_\epsilon, J_\eta, J_{\epsilon+\eta}$ by $\iota_\epsilon, \iota_\eta, \iota_{\epsilon+\eta}$ as in Notation 1.6.4. Let H_ϵ on J_ϵ be the pull back of any fixed hyperplane section on $\mathcal{K}_\epsilon$ and $H_{\epsilon+\eta}$ on $J_{\epsilon+\eta}$ be the pull back of any fixed hyperplane section on $\mathcal{K}_{\epsilon+\eta}$. We have the following lemma.

Lemma 5.2.7. *The divisors H_ϵ, $\phi^* H_{\epsilon+\eta}$ and $\iota^*_\epsilon(\phi^* H_{\epsilon+\eta})$ on J_ϵ are numerically equivalent.*

Proof. Since H_ϵ is the divisor on J_ϵ obtained by pulling back a hyperplane section on $K_\epsilon \subset \mathbb{P}^3$, $H_\epsilon \sim \phi_\epsilon^*(2\Theta)$. Similarly, $H_{\epsilon+\eta} \sim \phi_{\epsilon+\eta}^*(2\Theta)$. Recall $\phi = \phi_{\epsilon+\eta}^{-1} \circ \tau_P \circ \phi_\epsilon$. We get $\phi^* H_{\epsilon+\eta} \sim \phi_\epsilon^*(\tau_P^*(2\Theta))$ and $\iota_\epsilon^*(\phi^* H_{\epsilon+\eta}) \sim \iota_\epsilon^*(\phi_\epsilon^*(\tau_P^*(2\Theta))) = \phi_\epsilon^*([-1]^*(\tau_P^*(2\Theta)))$. By Remark 1.2.2, the divisors 2Θ and $\tau_P^*(2\Theta)$ are algebraically equivalent hence numerically equivalent, for any $P \in J$. Since isomorphisms preserve numerical equivalence, the divisors H_ϵ, $\phi^* H_{\epsilon+\eta}$ and $\iota_\epsilon^*(\phi^* H_{\epsilon+\eta})$ on J_ϵ are numerically equivalent.

□

We now state and prove the following theorem for computing the K-rational function g in the formula for $\langle \epsilon, \eta \rangle_{CT}$ in Theorem 5.1.1. Note that this theorem holds for any $P \in J$ and $\phi : J_\epsilon \to J_{\epsilon+\eta}$ depends on the choice of P. Later we will apply the theorem where P is the point on J corresponding to a K-rational point on $\mathcal{K}_\eta$ for the construction for g.

Theorem 5.2.8. *Let J be the Jacobian variety of a genus two curve $\mathcal{C}$ defined over a number field K. For $\epsilon, \eta \in Sel^2(J)$, let $(J_\epsilon, [2] \circ \phi_\epsilon), (J_\eta, [2] \circ \phi_\eta)$ and $(J_{\epsilon+\eta}, [2] \circ \phi_{\epsilon+\eta})$ denote the corresponding 2-coverings of J satisfying the commutative diagram in Lemma 5.1.6. Let $H_\epsilon = \theta_\epsilon^*\{x_1 = 0\}$ and $H_{\epsilon+\eta} = \theta_{\epsilon+\eta}^*\{c_1 y_1 + \ldots + c_4 y_4 = 0\}$ for $c_i \in K$ not all zero. Fix any $P \in J$. If*

$$g'(x_1, \ldots, x_4) = \mathcal{F}_{\epsilon,\eta}(x_1, \ldots, x_4; \theta_\eta \circ \phi_\eta^{-1}(P); c_1, \ldots, c_4),$$

then regarding $g = g'/x_1^2$ as a rational function on J_ϵ (via pull-back by θ_ϵ) we have

$$\mathrm{div}(g) = \phi^* H_{\epsilon+\eta} + \iota_\epsilon^*(\phi^* H_{\epsilon+\eta}) - 2H_\epsilon.$$

Proof. Step 1: We first prove the result when $P \notin J[4]$ and $c_1 y_1 + \ldots + c_4 y_4 = 0$ defines a general hyperplane on $\mathcal{K}_{\epsilon+\eta}$ avoiding the 16 singular points.

Taking $P_2 = \phi_\eta^{-1}(P)$ in Lemma 5.2.6, it follows that $g(P_1) = 0$ whenever $\theta_{\epsilon+\eta}(\phi(P_1)) \cdot c = 0$. Therefore, g vanishes on $\phi^* H_{\epsilon+\eta}$. Since $\theta_\epsilon \iota_\epsilon = \theta_\epsilon$, we know it must also vanish on $\iota_\epsilon^*(\phi^* H_{\epsilon+\eta})$. Also, by Lemma 5.2.2 and the definition of $\mathcal{F}_{\epsilon,\eta}$, we know g does not vanish on the whole of J_ϵ.

Consider the degree two morphism $\theta_{\epsilon+\eta} : J_{\epsilon+\eta} \to \mathcal{K}_{\epsilon+\eta}$. We know $\mathcal{K}_{\epsilon+\eta}$ taking away the 16 singular points is a smooth quasi-projective variety. By Bertini's Theorem, a general hyperplane section of $\mathcal{K}_{\epsilon+\eta}$ taking away the 16 singular points is smooth. Since $\mathcal{K}_{\epsilon+\eta}$ has dimension two and a hyperplane section is ample, we know it is connected by [Har77, Chapter III, Corollary 7.9] which implies that it is irreducible. Suppose D is a smooth irreducible hyperplane section on $\mathcal{K}_{\epsilon+\eta}$ that is away from the 16 singular points. Then we will show that $C = \theta_{\epsilon+\eta}^* D$ is irreducible. Suppose it is the union of more than one irreducible components. Since D is irreducible, the restriction of $\theta_{\epsilon+\eta}$ on each irreducible component of C is surjective on D. Since the degree of $\theta_{\epsilon+\eta}$ is two and there

are only finitely many interection points of the irreducible components of C, we get that the number of irreducible components of C is two. Moreover, the number of preimages on each of the irreducible componenets, denoted by C_1 and C_2, of a general point on D is one. We will show $C_1 \cong D \cong C_2$. If C_1 is smooth, then the restriction of $\theta_{\epsilon+\eta}$ gives a degree one morphism between smooth curves $C_1 \to D$, which is then an isomorphism. If C_1 is not smooth, then consider the composition of the blow up morphism of C_1 and the restriction of $\theta_{\epsilon+\eta}$ on C_1: $C_1' \to C_1 \to D$. We get the composition is a degree one morphism between two smooth curves, and so is an isomorphism. This implies that $D \to C_1' \to C_1$ is the inverse of $C_1 \to D$ and hence $C_1 \cong D$. Similarly we get that $C_2 \cong D$. Since $C \sim \phi_{\epsilon+\eta}^*(2\Theta)$, C is ample and hence connected. This implies that $\theta_{\epsilon+\eta}^{-1}(\theta_{\epsilon+\eta}(T)) = \{T\}$ for any $T \in C_1 \cap C_2$ and hence $\theta_{\epsilon+\eta}(T) \in D$ is one of the 16 singular points on $\mathcal{K}_{\epsilon+\eta}$. This contradicts with the assumption of D.

From the above discussion, we know that assuming $c_1y_1 + ... + c_4y_4 = 0$ gives a general hyperplane section on $\mathcal{K}_{\epsilon+\eta}$ avoiding the 16 singular points, $H_{\epsilon+\eta}$ is irreducible. Suppose $\phi^*H_{\epsilon+\eta} \neq \iota_\epsilon^*(\phi^*H_{\epsilon+\eta})$. We have

$$\mathrm{div}(g) = \phi^*H_{\epsilon+\eta} + \iota_\epsilon^*(\phi^*H_{\epsilon+\eta}) + E - 2H_\epsilon.$$

for some effective divisor E. Taking the intersection product with H_ϵ and using Lemma 5.2.7 shows that $E \cdot H_\epsilon = 0$. Since E is effective and H_ϵ is ample it follows that $E = 0$.

We will now show that $\iota_\epsilon^*(\phi^*H_{\epsilon+\eta}) = \phi^*H_{\epsilon+\eta}$ implies $P \in J[4]$ which completes the proof of the theorem for a general hyperplane section on $\mathcal{K}_{\epsilon+\eta}$ avoiding the 16 singular points and $P \notin J[4]$.

Suppose $\iota_\epsilon^*\phi^*H_{\epsilon+\eta} = \phi^*H_{\epsilon+\eta}$. We get $\phi_\epsilon^*\tau_P^*(2\Theta) \sim \iota_\epsilon^*\phi_\epsilon^*\tau_P^*(2\Theta)$. Since $\phi_\epsilon \circ \iota_\epsilon = [-1] \circ \phi_\epsilon$, this implies $\phi_\epsilon^*\tau_P^*(2\Theta) \sim \phi_\epsilon^*[-1]^*\tau_P^*(2\Theta)$ and hence $\tau_P^*(2\Theta) \sim [-1]^*\tau_P^*(2\Theta) \sim \tau_{-P}^*[-1]^*(2\Theta) \sim \tau_{-P}^*(2\Theta)$. So in this case, we derive $4P = 0$ as required.

Step 2: Suppose $P \notin J[4]$, we now show that the result holds for any hyperplane section on $\mathcal{K}_\eta$.

Consider $c = (c_1 : c_2 : c_3 : c_4)$ and wlog $c_1 \neq 0$. We assume $c_1 = 1$ and pass to the corresponding affine patch. Define $g_c = \mathcal{F}_{\epsilon,\eta}(x_1, ..., x_4; \theta_\eta \circ \phi_\eta^{-1}(P); c_1, ..., c_4)$. Let $D_c = \phi^*H_{\epsilon+\eta}$, which is the pull back on J_ϵ of the hyperplane section on $\mathcal{K}_{\epsilon+\eta}$ defined by the linear form with coefficient vector c. We know that $\mathrm{div}(g_c/x_1^2) = D_c + \iota_\epsilon^*D_c - 2H_\epsilon$ for a general $c \in \mathbb{A}^3$. Now we show that in fact the result holds for any $c \in \mathbb{A}^3$.

Let $c^0 \in \mathbb{A}^3$ satisfy $\mathrm{div}(g_{c^0}/x_1^2) = D_{c^0} + \iota_\epsilon^*D_{c^0} - 2H_\epsilon$. Treat y_i, the coordinates of $\mathcal{K}_{\epsilon+\eta}$, as functions on $J_{\epsilon+\eta}$. We have g_{c^0}/g_c is a rational function on $J_\epsilon \times \mathbb{A}^3$.

Define

$$h_c = \phi^*(\frac{\sum_{i=1}^4 c_i^0 y_i}{\sum_{i=1}^4 c_i y_i}) \cdot \iota_\epsilon^* \phi^*(\frac{\sum_{i=1}^4 c_i^0 y_i}{\sum_{i=1}^4 c_i y_i})$$

which is a well-defined nonzero rational function on $J_\epsilon \times \mathbb{A}^3$. For a general $c \in \mathbb{A}^3$, as functions on J_ϵ, we have $\operatorname{div}(g_{c^0}/g_c) = D_{c^0} + \iota_\epsilon^* D_{c^0} - D_c - \iota_\epsilon^* D_c$ and

$$\operatorname{div}(g_{c^0}/g_c) = \operatorname{div}(h_c). \tag{5.2.1}$$

Hence, define λ such that $\lambda h_c = g_{c^0}/g_c$, which makes λ a well-defined rational function on $J_\epsilon \times \mathbb{A}^3$. Moreover, we know $\lambda(-, c)$ is a constant function on J_ϵ for $c \in U \subset \mathbb{A}^3$ and U is open. It suffices to show that $\lambda(-, c)$ is a constant function on J_ϵ for any $c \in \mathbb{A}^3$. Consider the following commutative diagram.

$$\begin{array}{ccc} J_\epsilon \times U & \xrightarrow{inc} & J_\epsilon \times \mathbb{A}^3 \\ \downarrow & & \downarrow \\ U & \xrightarrow{inc} & \mathbb{A}^3, \end{array}$$

where each vertical map is the projection to the second component. Consider the induced commutative diagram of the corresponding function fields. Define $m(c) = \lambda(T, c)$ in $K(U)$ for a fixed $T \in J_\epsilon$ and any $c \in U$. Then the image of m in $K(J_\epsilon \times U)$ is $\lambda|_{J_\epsilon \times U}$ and hence the image of m in $K(J_\epsilon \times \mathbb{P}^3)$ is λ. The fact that λ is also the image of the corresponding element of m in $K(\mathbb{P}^3)$ shows that λ is a constant function given any second input $c \in \mathbb{A}^3$ as required.

Step 3: Lastly, we show that the result holds for any $P \in J$. Consider $c_i \in K$ not all zero. Let $g_P = \mathcal{F}_{\epsilon,\eta}(x_1, ..., x_4; \theta_\eta \circ \phi_\eta^{-1}(P); c_1, ..., c_4)$ and $\phi_P = \phi_{\epsilon+\eta}^{-1} \circ \tau_P \circ \phi_\epsilon$. Suppose $H_{\epsilon+\eta} = \theta_{\epsilon+\eta}^* \{c_1 y_1 + \ldots + c_4 y_4 = 0\}$. We have $\operatorname{div}(g_P/x_1^2) = \phi_P^* H_{\epsilon+\eta} + \iota_\epsilon^* \phi_P^* H_{\epsilon+\eta} - 2H_\epsilon$ for general $P \in J$. We now show that in fact the result holds for any $P \in J$.

Fix a general $P_0 \in J$ satisfying the equation above. We know g_{P_0}/g_P is a rational function on $J_\epsilon \times J$. For a general $P \in J$, the following holds as functions on J_ϵ

$$\operatorname{div}(g_{P_0}/g_P) = \operatorname{div}(h_P)$$

where $h_P = \frac{\phi_{P_0}^*(\sum_{i=1}^4 c_i y_i)}{\phi_P^*(\sum_{i=1}^4 c_i y_i)} \cdot \iota_\epsilon^* \frac{\phi_{P_0}^*(\sum_{i=1}^4 c_i y_i)}{\phi_P^*(\sum_{i=1}^4 c_i y_i)}$.

It suffices to prove that h_P is a well-defined nonzero rational function on $J_\epsilon \times J$, then the rest of the proof is the same as in Step 2. However, this naturally follows from the fact that: for any f rational function on J, $(Q, P) \mapsto f(Q + P)$ is a well-defined rational function on $J \times J$.

□

Recall that the condition of Theorem 5.1.1 is that there exists a K-rational point $R \in \mathcal{K}_\eta$ and the field of definition of the preimages of R is $K(\sqrt{a})$ for some nonzero $a \in K$. Let $Q \in J_\eta$ be a preimage of $R \in \mathcal{K}_\eta(K)$. Consider $\phi = \mu(-, Q)$, which is defined over $K(\sqrt{a})$ as shown in Corollary 5.1.7. By Remark 5.1.8, we assume $[K(Q) : K] = 2$ and we need to construct a K-rational function g whose divisor of zeros and poles is $\phi^*(H_{\epsilon+\eta}) + \sigma(\phi^*(H_{\epsilon+\eta})) - 2H_\epsilon$, where H_ϵ on J_ϵ is the pull back of some fixed hyperplane section on $\mathcal{K}_\epsilon$, $H_{\epsilon+\eta}$ on $J_{\epsilon+\eta}$ is the pull back of some fixed hyperplane section on $\mathcal{K}_{\epsilon+\eta}$ and $G_{K(Q)/K} = \{1, \sigma\}$.

Lemma 5.2.9. *If $G_{K(Q)/K} = \{1, \sigma\}$, then*

$$\sigma(\phi) = \iota_{\epsilon+\eta} \circ \phi \circ \iota_\epsilon.$$

Proof. From the definition of $\mu : J_\epsilon \times J_\eta \to J_{\epsilon+\eta}$, we get $\mu(\iota_\epsilon(T_1), \iota_\eta(T_2)) = \iota_{\epsilon+\eta}(\mu(T_1, T_2))$ for any $T_1 \in J_\epsilon$ and any $T_2 \in J_\eta$. Since $\sigma(Q) = \iota_\eta(Q)$, we have $\iota_{\epsilon+\eta} \circ \phi \circ \iota_\epsilon(T) = \iota_{\epsilon+\eta}(\mu(\iota_\epsilon(T), Q)) = \mu(T, \iota_\eta(Q)) = \mu(T, \sigma(Q)) = \sigma(\phi)(T)$, for any $T \in J_\epsilon$.

□

Remark 5.2.10. It is immediate from Lemma 5.2.9 that $\sigma(\phi^* H_{\epsilon+\eta}) = \iota_\epsilon^*(\phi^* H_{\epsilon+\eta})$.

Corollary 5.2.11. *Suppose $G_{K(Q)/K} = \{1, \sigma\}$. Let $H_\epsilon = \theta_\epsilon^*\{x_1 = 0\}$ and $H_{\epsilon+\eta} = \theta_{\epsilon+\eta}^*\{c_1 y_1 + \ldots + c_4 y_4 = 0\}$ for $c_i \in K$ not all zero. Define*

$$g'(x_1, \ldots, x_4) = \mathcal{F}_{\epsilon,\eta}(x_1, \ldots, x_4; R; c_1, \ldots, c_4).$$

Then regarding $g = g'/x_1^2$ as a K-rational function on J_ϵ (via pull-back by θ_ϵ), we have

$$\operatorname{div}(g) = \phi^* H_{\epsilon+\eta} + \sigma(\phi^* H_{\epsilon+\eta}) - 2H_\epsilon.$$

Proof. The result follows from applying Theorem 5.2.8 with $P = \phi_\eta(Q)$ and Remark 5.2.10.

□

Now we describe a method for pulling back g via $J_\epsilon \xrightarrow{\theta_\epsilon} \mathcal{K}_\epsilon$. This is almost identical to the discussion in Section 4.2.2, but we still include it here for completeness.

Recall, by Theorem 1.11.1, we have an explicit isomorphism $J_\epsilon \subset \mathbb{P}^{15} \xrightarrow{\phi_\epsilon} J \subset \mathbb{P}^{15}$ and we let $u_0, ..., u_9, v_1, ..., v_6$ denote the coordinates of the ambient space of $J_\epsilon \subset \mathbb{P}^{15}$, $k_{11}, k_{12}, ..., k_{44}, b_1, ..., b_6$ denote the coordinates of the ambient space of $J \subset \mathbb{P}^{15}$. Moreover, ϕ_ϵ is represented by a block diagonal matrix consisting of a block of size 10 corresponding to the even basis elements and a

block of size 6 corresponding to the odd basis elements. By the naive method described in Section 3.2, we compute an explicit isomorphism $\mathcal{K}_\epsilon \subset \mathbb{P}^3 \xrightarrow{\psi_\epsilon} \mathcal{K} \subset \mathbb{P}^3$ corresponding to ϵ. More specifically, we know $\phi_\epsilon(\phi_\epsilon^{-1})^\sigma = \tau_{\epsilon_\sigma}$ and $\psi_\epsilon(\psi_\epsilon^{-1})^\sigma$ is the action of translation by $\epsilon'_\sigma \in J[2]$ on $\mathcal{K} \subset \mathbb{P}^3$ such that $(\sigma \mapsto \epsilon_\sigma), (\sigma \mapsto \epsilon'_\sigma)$ both represent $\epsilon \in \mathrm{Sel}^2(J)$. By potentially replacing ψ_ϵ with ψ'_ϵ such that $\psi'_\epsilon\psi_\epsilon^{-1}$ is the action of translation by some suitable $T \in J[2]$, we can assume $\epsilon_\sigma = \epsilon'_\sigma$ for any $\sigma \in G_K$.

The isomorphism $\psi_\epsilon : \mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ induces a natural isomorphism $\tilde{\psi}_\epsilon : \mathbb{P}^9 \to \mathbb{P}^9$. More explicitly, suppose ψ_ϵ is represented by the 4×4 matrix A where $(k'_1 : ..., k'_4) \mapsto (\sum_{i=1}^4 A_{1i}k'_i : ... : \sum_{i=1}^4 A_{4i}k'_i)$. Define $k'_{ij} = k'_ik'_j$. Then $\tilde{\psi}_\epsilon : \mathbb{P}^9_{k'_{ij}} \to \mathbb{P}^9_{k_{ij}}$ is given by $(k'_{11} : k'_{12} : ... : k'_{44}) \mapsto (\sum_{i,j=1}^4 A_{1i}A_{1j}k'_{ij} : \sum_{i,j=1}^4 A_{1i}A_{2j}k'_{ij} : ... : \sum_{i,j=1}^4 A_{4i}A_{4j}k'_{ij})$. On the other hand, the isomorphism $\phi_\epsilon : J_\epsilon \subset \mathbb{P}^{15}_{\{u_i,v_i\}} \to J \subset \mathbb{P}^{15}_{\{k_{ij},b_i\}}$ induces a natural isomorphism $\tilde{\phi}_\epsilon : \mathbb{P}^9_{u_i} \to \mathbb{P}^9_{k_{ij}}$ which is simply represented by the 10×10 block of the matrix representing ϕ_ϵ. Since $\epsilon_\sigma = \epsilon'_\sigma$ for all $\sigma \in G_K$, we actually have $\tilde{\phi}_\epsilon((\tilde{\phi}_\epsilon)^{-1})^\sigma = \tilde{\psi}_\epsilon((\tilde{\phi}_\epsilon)^{-1})^\sigma$. Therefore, we get $(\tilde{\psi}_\epsilon)^{-1}\tilde{\phi}_\epsilon$ defined over K and the following commutative diagram that decomposes the standard diagram (1.6.2):

$$\begin{array}{ccccccc}
J_\epsilon \subset \mathbb{P}^{15}_{\{u_i,v_i\}} & \xrightarrow{proj} & \mathbb{P}^9_{u_i} & \xrightarrow{(\tilde{\psi}_\epsilon)^{-1}\tilde{\phi}_\epsilon} & \mathbb{P}^9_{k'_{ij}} & \xrightarrow{g_2} & \mathcal{K}_\epsilon \subset \mathbb{P}^3_{k'_i} \\
\downarrow{\scriptstyle \phi_\epsilon} & & & \searrow^{\tilde{\phi}_\epsilon} \quad \swarrow_{\tilde{\psi}_\epsilon} & & & \downarrow{\scriptstyle \psi_\epsilon} \\
J \subset \mathbb{P}^{15}_{\{k_{ij},b_i\}} & \xrightarrow{proj} & & \mathbb{P}^9_{k_{ij}} & \xrightarrow{g_1} & & \mathcal{K} \subset \mathbb{P}^3_{k_i},
\end{array} \tag{5.2.2}$$

where $g_1 : (k_{11} : ... : k_{44}) \mapsto (k_{11} : ... : k_{14})$ and $g_2 : (k'_{11} : ... : k'_{44}) \mapsto (k'_{11} : ... : k'_{14})$ are the natural projection maps. The composition of the morphisms on the bottom gives the standard morphism $J \xrightarrow{|2\Theta|} \mathcal{K} \subset \mathbb{P}^3$ and the composition of the morphisms on the top gives $J_\epsilon \xrightarrow{\theta_\epsilon} \mathcal{K}_\epsilon \subset \mathbb{P}^3$ representing the morphism induced by $|\phi_\epsilon^*(2\Theta)|$.

We observe the following two remarks.

Remark 5.2.12. From Corollary 5.2.11 and the discussion above, we know that the K-rational function g constructed in the formula for the Cassels-Tate pairing is a quotient of two linear forms on $J_\epsilon \subset \mathbb{P}^{15}$. Moreover, by the construction for g and the formula for the Cassels-Tate pairing in Theorem 5.1.1, we note the denominator of $g(P_v)$ is a always a square for any $P_v \in J_\epsilon(K_v)$ and so we can replace g by its numerator in the computation.

Remark 5.2.13. From the above discussion and diagram (5.2.2), given a point $R \in \mathcal{K}_\epsilon(K) \subset \mathbb{P}^3_{k'_i}$, we can compute its corresponding image $(u_0 : ... : u_9) \in \mathbb{P}^9_{u_i}$. Then following the discussion at the end of Section 1.11, we can compute a

nonzero $a \in K$ such that the field of definition of the preimages of R in J_ϵ is $K(\sqrt{a})$. Moreover, they are defined over K if and only if $K(\sqrt{a}) = K$. The same result holds when replacing K with K_v, for any place v of K.

5.3 Equations Satisfied by V_P

We initially investigated the results in this section as we thought they are needed in the computation for the Cassels-Tate pairing. However, it turned out that they are not needed. We still include these results here as they describe some properties of the $(2,2,2)$-form $\mathcal{F}$ and might be useful for other related research questions.

As discussed in Section 1.3.2, the morphism $J \xrightarrow{|2\Theta|} \mathcal{K} \subset \mathbb{P}^3$ denotes the map $P \mapsto k(P)$, where $k(P) = (k_1(P) : k_2(P) : k_3(P) : k_4(P)) \in \mathbb{P}^3$ and $k_1, ..., k_4$ form a basis for $\mathcal{L}(\Theta^+ + \Theta^-)$. Fix $P \in J$. We define the image of the morphism $Q \mapsto (k(Q), k(P+Q))$ in $\mathbb{P}^3 \times \mathbb{P}^3$:

$$V_P = \mathrm{Im}\left(J \xrightarrow{|2\Theta| \times |\tau_P^*(2\Theta)|} \mathbb{P}^3 \times \mathbb{P}^3 \right).$$

In the special case where $P \in J[2]$, we observe $V_P = \{(k(Q), M_P k(Q)), P \in J\}$, where $M_P \in \mathrm{GL}_4(\bar{K})$ represents the action of translation by P on $\mathcal{K} \subset \mathbb{P}^3$. This implies that $V_P \cong \mathcal{K}$. In the case where $P \notin J[2]$, we check that V_P bijects with J set-theoretically.

In this section, we will study the equations satisfied by V_P as well as the defining equations of V_P. By the reason above, we are interested in the case where $P \notin J[2]$. We will show how the equations satisfied by V_P are related to the $(2,2,2)$-form $\mathcal{F}$ constructed in Lemma 5.2.1.

5.3.1 (i,j)-forms vanishing on V_P

Let i, j be positive integers and S_{ij} be the vector space of (i,j)-forms vanishing on V_P. Consider the following natural linear maps:

$$l_{ij} : S^i\mathcal{L}(2\Theta) \otimes S^j\mathcal{L}(\tau_P^*(2\Theta)) \to \mathcal{L}(2i\Theta + \tau_P^*(2j\Theta)),$$

such that $l_{ij}(f \otimes g) = fg$ for any $f \in S^i\mathcal{L}(2\Theta), g \in S^j\mathcal{L}(\tau_P^*(2\Theta))$. Note that we let S^kV denote the symmetric product of order k of the vector space V.

By Section 1.3.1, we know $\dim \mathcal{L}(2i\Theta) = 4i^2$. We compute $\dim S^i\mathcal{L}(2\Theta) = \binom{i+3}{3}$. Since $2i\Theta + \tau_P^*(2j\Theta) \sim \tau_S^*(2(i+j)\Theta)$ for $S \in J$ such that $jP = (i+j)S$, we get $\dim \mathcal{L}(2i\Theta + \tau_P^*(2j\Theta)) = 4(i+j)^2$. This implies that $\dim \mathrm{Im}\, l_{ij} \leq 4(i+j)^2$. Recall $2n\Theta \sim n(\Theta^+ + \Theta^-)$. By construction, we have $\dim S_{ij} = \dim \ker l_{ij}$ which implies $\dim S_{ij} \geq \binom{i+3}{3}\binom{j+3}{3} - 4(i+j)^2$. Moreover, each of these inequalities is an equality if and only if the corresponding l_{ij} is surjective. We first quote the

following lemma.

Lemma 5.3.1. *Let P_1, P_2 be two points on J. Suppose the theta divisor Θ corresponds to $\{\omega_0\}\times\mathcal{C}+\mathcal{C}\times\{\omega_0\}$ on $\mathcal{C}\times\mathcal{C}$ with ω_0 a fixed choice of Weierstrass point on C. Consider the following natural map for $i, j \geq 2$ positive integers:*

$$\mathcal{L}(\tau_{P_1}^*(i\Theta)) \otimes \mathcal{L}(\tau_{P_2}^*(j\Theta)) \xrightarrow{\alpha_{ij}} \mathcal{L}(\tau_{P_1}^*(i\Theta) + \tau_{P_2}^*(j\Theta)).$$

We have that

(i) if $i > 2$ or $j > 2$, then α_{ij} is surjective;

(ii) α_{22} is surjective if and only if $\{R \in J[2] : P_1 - P_2 \in \Theta + R\} = \emptyset$.

Proof. (i)[BL04, Proposition 7.3.4]. (ii)[PP04, Theorem 5.8]

□

Corollary 5.3.2. *Let $T = \{\Theta_\omega + R : R \in J[2],\ \omega$ is a Weierstrass point$\}$. $\dim S_{11} = 0$ if and only if $P \notin T$. In particular, for a general point $P \in J$, $\dim S_{11} = 0$*

Proof. Apply Lemma 5.3.1(ii) in the case $P_1 = \mathcal{O}_J$ and $P_2 = P$ with a fixed choice of Weierstrass point ω_0. We can see $P \notin T$ if and only if $\{R \in J[2] : -P \in \Theta_{\omega_0} + R\} = \emptyset$ which is if and only if l_{11} is surjective. In this case, l_{11} is also injective which implies that $\dim S_{11} = \dim\ker l_{11} = 0$.

□

Proposition 5.3.3. *If $\dim S_{11} = 0$, then l_{mn} is surjective which gives*

$$\dim S_{mn} = \binom{m+3}{3}\binom{n+3}{3} - 4(m+n)^2,$$

for all $m, n \geq 1$.

Proof. Recall that $\dim S_{mn} = \dim\ker l_{mn}$, with l_{mn} defined as

$$l_{mn} : S^m\mathcal{L}(2\Theta) \otimes S^n\mathcal{L}(\tau_P^*(2\Theta)) \to \mathcal{L}(2m\Theta + \tau_P^*(2n\Theta)),$$

where $l_{mn}(f \otimes g) = fg$ for any $f \in S^m\mathcal{L}(2\Theta), g \in S^n\mathcal{L}(\tau_P^*(2\Theta))$.

By hypothesis $\dim S_{11} = 0$, this map is surjective when $(m, n) = (1, 1)$. Our claim is that it is surjective for all $m, n \geq 1$ and we will prove it by induction.

To prove the result when $(m, n) = (i+1, j)$ given that the result holds when $(m, n) = (i, j)$, we consider the commutating diagram

$$\begin{array}{ccc} S^i\mathcal{L}(2\Theta)\otimes S^j\mathcal{L}(\tau_P^*(2\Theta))\otimes\mathcal{L}(2\Theta) & \xrightarrow{h_1} & S^{i+1}\mathcal{L}(2\Theta)\otimes S^j\mathcal{L}(\tau_P^*(2\Theta)) \\ \downarrow v & & \downarrow l_{(i+1)j} \\ \mathcal{L}(2i\Theta+\tau_P^*(2j\Theta))\otimes\mathcal{L}(2\Theta) & \xrightarrow{h_2} & \mathcal{L}(2(i+1)\Theta+\tau_P^*(2j\Theta)) \end{array}$$

where $h_1 : x\otimes y\otimes z\mapsto xz\otimes y, v : x\otimes y\otimes z\mapsto xy\otimes z$ and $h_2 : x\otimes y\mapsto xy$.

We have v surjective by induction hypothesis. To show the surjectivity of h_2, we replace $2i\Theta+\tau_P^*(2j\Theta)$ by a linearly equivalent divisor $(i+j)\tau_Q^*(2\Theta)$ where $jP=(i+j)Q$ and apply Lemma 5.3.1(i). A diagram chase shows that $l_{(i+1)j}$ is surjective as required.

□

Remark 5.3.4. For completeness, we note l_{mn} is surjective for $(m,n)=(0,0),(1,0)$ or $(0,1)$, but not surjective for $(m,n)=(d,0)$ or $(0,d)$ with $d\geq 2$.

5.3.2 Partials of the (2, 2, 2)-form $\mathcal{F}$

In this section, we suppose $P\notin J[2]$ and we will construct 4 linearly independent $(2,1)$-forms and 4 linearly independent $(1,2)$-forms vanishing on V_P. In the case where $\dim S_{11}=0$, with criteria given in Corollary 5.3.2, these span S_{21} and S_{12} by Proposition 5.3.3. We first have the following definition from [CF96, Chapter 4, Section 0].

Definition 5.3.5. *The dual of the Kummer surface* $\mathcal{K}$ is a quartic surface in $\mathbb{P}^3$ that parameterizes $\mathrm{Pic}^3(\mathcal{C})$ modulo the involution induced by the involution on the genus two curve $\mathcal{C}$. It is denoted by $\mathcal{K}^*$.

Remark 5.3.6. It is explained in [CF96, Chapter 4, Sections 3 and 4] that $\mathcal{K}^*$ is in fact the projective dual of $\mathcal{K}$. Recall $k(P)=(k_1(P):...:k_4(P))\in\mathcal{K}\subset\mathbb{P}^3$ for any $P\in J$ and the quartic defining equation of $\mathcal{K}$ is denoted by $G(k_1,...,k_4)$ as in Section 1.3.2. We therefore define $k^*(P)=(k_1^*(P):...:k_4^*(P))\in\mathcal{K}^*\subset\mathbb{P}^3$, where $k_i^*(P)=\partial G/\partial x_i(k(P))$ and $P\in J\setminus J[2]$.

In Lemma 5.2.1, we constructed explicitly

$$\mathcal{F}(x,y,z)=\sum_{i,j=1}^{4}\psi_{ij}(x,y)z_iz_j$$

where the ψ_{ij}, defined in Corollary 1.3.7, are $(2,2)$-forms satisfying

$$\psi_{ij}(k(Q),k(P+Q))=c(P,Q)\big(k_i(P)k_j(P+2Q)+k_j(P)k_i(P+2Q)\big) \quad (5.3.1)$$

for all $P, Q \in J$ and some rational function $c(P, Q)$ on $J \times J$ independent of i, j. Note $c(P, Q) = \lambda(Q, P + Q)$ where λ is defined in the beginning of Section 5.2.1. Since $\sum_{i=1}^{4} k_i(P)k_i^*(P) = 0$ for $P \in J \setminus J[2]$, by Lemma 5.2.1, we know that

$$\mathcal{F}(k(Q), k(P + Q), k^*(P)) = 0,$$

for all $P \in J \setminus J[2], Q \in J$.

Let $T_P J$ be the tangent space at $P \in J$. This is a 2-dimensional vector space defined intrinsically. If the rational map $k : J \to \mathbb{A}^4$ is regular at P, then it has a well-defined derivative, which is a linear map

$$dk(P) : T_P J \to \mathbb{A}^4$$

with image contained in the affine cone over $T_{k(P)}\mathcal{K} \subset \mathbb{P}^3$. Therefore

$$\sum_{i=1}^{4} (dk(P)(v))_i k_i^*(P) = 0 \tag{5.3.2}$$

for all $v \in T_P J$.

We have the following proposition.

Proposition 5.3.7. *The 4 $(1, 2, 2)$-forms and 4 $(2, 1, 2)$-forms derived from taking partials of the $(2, 2, 2)$-form $\mathcal{F}$ with respect to the first and second sets of coordinates vanish at $(k(Q), k(P + Q), k^*(P))$ for all $P \in J \setminus J[2], Q \in J$.*

Proof. Fix $Q \in J$, $i, j \in \{1, ..., 4\}$ and view each side of (5.3.1) as a function of $P \in J$. The left hand side of the equation, denoted by $L(P)$, is the composition of the following:

$$J \xrightarrow{\tau_Q} J \xrightarrow{k} \mathbb{A}^4 \xrightarrow{\psi_{ij,Q}} \mathbb{A}^1,$$

where $\mathcal{K} \xrightarrow{\psi_{ij,Q}} \mathbb{A}$ maps $a = (a_1, a_2, a_3, a_4)$ to $\psi_{ij}(k(Q), a)$.

Hence, via taking derivative of $L(P)$ and applying chain rule, we get

$$\begin{aligned} dL(P) &= d\psi_{ij,Q}(k(P + Q)) \circ dk(P + Q) \circ d\tau_Q(P) \\ &= \Big(\sum_{r=1}^{4} \frac{\partial \psi_{ij}}{\partial y_r}(k(Q), k(P + Q)) \cdot dk_r(P + Q) \Big) \circ d\tau_Q(P). \end{aligned}$$

On the other hand, denote the right hand side of (5.3.1) by $R(P)$. We get

$$\begin{aligned} dR(P) = {} & dc(P,Q)\big(k_i(P)k_j(P+2Q) + k_j(P)k_i(P+2Q)\big) \\ & + c(P,Q)\big(k_j(P+2Q)dk_i(P) + k_i(P+2Q)dk_j(P) \\ & + k_i(P)dk_j(P+2Q)d\tau_{2Q}(P) + k_j(P)dk_i(P+2Q)d\tau_{2Q}(P)\big). \end{aligned}$$

By $\sum_{i=1}^4 k_i(P)k_i^*(P) = 0$ and (5.3.2), we deduce that

$$\sum_{i=1}^4\sum_{j=1}^4 k_i^*(P)k_j^*(P)dL(P)(v) = \sum_{i=1}^4\sum_{j=1}^4 k_i^*(P)k_j^*(P)dR(P)(v) = 0,$$

for any $v \in T_P J$. This implies that $\sum_{i=1}^4\sum_{j=1}^4 k_i^*(P)k_j^*(P)dL(P) : T_P J \to \mathbb{A}^1$ is the zero map. Since the map $k : J \mapsto \mathbb{A}^4$ is local diffeomorphism around a general point on J, for general $P \in J$ and any $w \in T_{k(P+Q)}\mathcal{K}$, there exists $w' \in T_P J$ such that $dk(P+Q) \circ d\tau_Q(P)(w') = w$. Therefore,

$$\begin{aligned} & \sum_{i=1}^4\sum_{j=1}^4 k_i^*(P)k_j^*(P)\sum_{r=1}^4 \frac{\partial \psi_{ij}}{\partial y_r}(k(Q),k(P+Q))\cdot w_r \\ =& \sum_{i=1}^4\sum_{j=1}^4 k_i^*(P)k_j^*(P)\Big(\sum_{r=1}^4 \frac{\partial \psi_{ij}}{\partial y_r}(k(Q),k(P+Q))\cdot dk_r(P+Q)\Big)\circ d\tau_Q(P)(w') \\ =& 0. \end{aligned}$$

Hence, we it can be checked that

$$\frac{\partial \mathcal{F}}{\partial y_r}(k(Q),k(P+Q),k^*(P)) = h(P,Q)k_r^*(P+Q) \tag{5.3.3}$$

where h is a rational function on $J \times J$, independent of $r = 1,\ldots,4$.

To show that the 4 $(2,1,2)$-forms derived from taking partials of $\mathcal{F}$ with respect to the second sets of coordinates vanish at $(k(Q),k(P+Q),k^*(P))$ for all $P,Q \in J$, it suffices to show they vanish at $(k(Q),k(P+Q),k^*(P))$ for general $P,Q \in J$. Hence, it suffices to show that h is identically zero. Then since the $(2,2,2)$-form $\mathcal{F}$ is symmetric in the first two sets of variables, we obtain $\partial\mathcal{F}/\partial x_i(x,y,z)$ by swapping x and y in $\partial\mathcal{F}/\partial y_i(x,y,z)$. Hence,

$$\begin{aligned} & \partial\mathcal{F}/\partial x_i(k(Q),k(P+Q),k^*(P)) \\ =& \partial\mathcal{F}/\partial x_i(k(-Q),k(-P-Q),k^*(P)) \\ =& \partial\mathcal{F}/\partial y_i(k(-P-Q),k(-Q),k^*(P)) \\ =& 0, \end{aligned}$$

which implies the 4 $(1,2,2)$-forms also vanish at $(k(Q),k(P+Q),k^*(P))$, for any $P,Q \in J$.

Suppose that h is nonzero. We will derive a contradiction by fixing $P \in J \setminus J[4]$ and viewing each side of (5.3.3) as a rational function of $Q \in J$.

We know $\{k_1, k_2, k_3, k_4\}$ is a basis for $\mathcal{L}(\Theta^+ + \Theta^-)$. Since the defining equation of $\mathcal{K}$, denoted by G, is a homogeneous quartic polynomial, we get $k_i^* = \partial G/\partial k_i(k_1, \ldots, k_4) \in \mathcal{L}(3\Theta^+ + 3\Theta^-)$. Now we equate the divisors of zeros and poles of each side of (5.3.3) we obtain

$$D_r - 2(\Theta^+ + \Theta^-) - \tau_P^*(\Theta^+ + \Theta^-) = \mathrm{div}(h) + D_r' - 3\tau_P^*(\Theta^+ + \Theta^-)$$

where $D_1, \ldots, D_4$ and $D_1', \ldots, D_4'$ are effective divisors on J. This implies that

$$\mathrm{div}(h) - 2(\tau_P^*(\Theta^+ + \Theta^-) - (\Theta^+ + \Theta^-)) = D_r - D_r'$$

for all $r = 1, ..., 4$.

Recall even elements in $\mathcal{L}(2\Theta^+ + 2\Theta^-)$ are spanned by $k_i k_j$ with $i, j = 1, ..., 4$ and it can be checked that $k_1 \nmid k_r^*$ as polynomials for any $r = 1, ..., 4$. Writing $k_r^* = k_1 h_{r,1}(k_1, k_2, k_3, k_4) + h_{r,2}(k_2, k_3, k_4)$ with $h_{r,1}$ homogeneous polynomial of degree 2 and $h_{r,2}$ homogeneous polynomial of degree 3, we get that $k_1 h_{r,1}(k_1, k_2, k_3, k_4) \in \mathcal{L}(2\Theta^+ + 2\Theta^-)$ and $h_{r,2}(k_2, k_3, k_4) \in \mathcal{L}(3\Theta^+ + 3\Theta^-) \setminus \mathcal{L}(2\Theta^+ + 2\Theta^-)$. Also because $h_{r,2}(k_1, k_2, k_3, k_4)$ is even, we know it has a pole at $P \in J$ if and only if it has a pole at $-P$. This implies that the divisor of poles of $h_{r,2}(k_2, k_3, k_4)$ is precisely $3\Theta^+ + 3\Theta^-$ and D_r' is the divisor of zeros of k_r^*. Since the Kummer surface has only 16 singular points and points on the common components of D_r' are singular points by definition. We deduce that the divisors $D_1', \ldots, D_4'$ have no common components. This implies that $\mathrm{div}(h) - 2\big(\tau_P^*(\Theta^+ + \Theta^-) - (\Theta^+ + \Theta^-)\big)$ is effective. By Remark 1.2.2, we know $\mathrm{div}(h) - 2\big(\tau_P^*(\Theta^+ + \Theta^-) - (\Theta^+ + \Theta^-)\big)$ is algebraically equivalent to zero, and hence numerically equivalent to zero. Therefore, $\mathrm{div}(h) = 2\big(\tau_P^*(\Theta^+ + \Theta^-) - (\Theta^+ + \Theta^-)\big) \sim \tau_P^*(4\Theta) - 4\Theta$, which contradicts with $P \notin J[4]$.

□

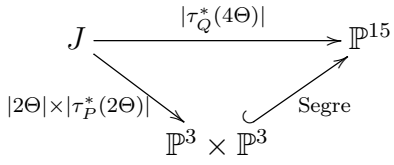
Remark 5.3.8. Let $x = (x_1, ..., x_4), y = (y_1, ..., y_4)$. For $P \in J \setminus J[2]$, let $k^*(P) = (k_1^*(P), ..., k_4^*(P))$ and define $\mathcal{F}_P(x, y) = \mathcal{F}(x, y, k^*(P))$. Then $\mathcal{F}_P(x, y)$ is a $(2, 2)$-form vanishing on V_P. By Proposition 5.3.7, its partial derivatives, which are 4 linearly independent $(2, 1)$-forms and 4 linearly independent $(1, 2)$-forms, also vanish on V_P.

5.3.3 Defining equations of V_P

It would be interesting to determine the bi-degrees of a set of polynomials sufficient to define V_P set-theoretically. We give an answer in the next lemma in the case $\dim S_{11} = 0$.

Lemma 5.3.9. *If* $\dim S_{11} = 0$, *then* V_P *is defined by* $(2, 2)$*-forms.*

Proof. Let $f_1, \dots, f_4$ and $g_1, \dots, g_4$ be bases for $\mathcal{L}(2\Theta)$ and $\mathcal{L}(\tau_P^*(2\Theta))$ respectively. Then the 16 elements $f_i g_j \in \mathcal{L}(2\Theta + \tau_P^*(2\Theta))$ are linearly independent by our assumption $\dim S_{11} = 0$. For $Q \in J$ such that $P = 2Q$, we have $2\Theta + \tau_P^*(2\Theta) \sim \tau_Q^*(4\Theta)$. Via the commutating diagram



and the fact that $J \subset \mathbb{P}^{15}$ is defined by quadratic forms by [Mum69, Theorem 10], we deduce that $V_P \subset \mathbb{P}^3 \times \mathbb{P}^3$ is defined by $(2,2)$-forms.

□

A further question would be to determine the bi-degrees of a generating set for the bi-homogeneous ideal $I(V_P) \subset K[x_1, \dots, x_4; y_1, \dots, y_4]$. However, we will not address it in this thesis.

5.4 Prime Bound

In this section, we show that the formula for the Cassels-Tate pairing in Theorem 5.1.1 is always a finite product. Moreover, there exists a computable bound for each pair of Selmer elements (ϵ, η) such that for a place of K whose norm is a power of a prime above the bound, the local Cassels-Tate pairing between ϵ and η is trivial, as mentioned in Remark 5.1.2. The argument is very similar to Section 4.4 and we have $S = \{\text{places of bad reduction for } \mathcal{C}\} \cup \{\text{places dividing } 2\} \cup \{\text{infinite places}\}$.

Recall we assume $\mathcal{K}_\eta$, the twisted Kummer surface corresponding to η, has a K-rational point R. There exists a computable nonzero $a \in K$, such that the field of definition of the preimages of R on J_η is $K(\sqrt{a})$ as explained in Section 1.11. As discussed in Remark 5.1.8, $\langle \epsilon, \eta \rangle_{CT}$ is trivial if $K(\sqrt{a}) = K$. Suppose $K(\sqrt{a})$ is a quadratic extension of K. By Corollary 5.2.11, we can compute a rational function g on J_ϵ, which is a quotient of two linear forms denoted by l_1, l_2 on $J_\epsilon \subset \mathbb{P}^{15}$ as discussed in Remark 5.2.12, such that

$$\langle \epsilon, \eta \rangle_{CT} = \prod_v (g(P_v), a)_v.$$

Recall that $(\ ,\ )_v$ denotes the Hilbert Symbol for a given place v of K and P_v is any local point on J_ϵ avoiding the zeros and poles of g. By Lemma 1.4.18, it suffices to find a finite set S_1, a set of places of K containing S, such that both arguments of the Hilbert symbol in the formula for $\langle \epsilon, \eta \rangle_{CT}$ have valuation 0 for any $v \notin S_1$. Hence, it suffices to choose a subset S_1 that contains the places of K that divide a and solves Problem 4.4.1 in the case $n = 2$.

Suppose $(a_1, ..., a_6)$ represents the image of ϵ in $L^*/(L^*)^2K^*$ with $L = K[x]/(f)$ as described in Section 1.10.1. By Theorem 1.11.1, we have an explicit formula for the linear isomorphism ϕ_ϵ

$$J_\epsilon \subset \mathbb{P}^{15} \xrightarrow{\phi_\epsilon} J \subset \mathbb{P}^{15},$$

which is defined over $K' = L_1(\sqrt{a_1}, ..., \sqrt{a_6})$ with L_1 denoting the splitting field of f. Let $M_\epsilon \in \mathrm{GL}_{16}(K')$ represent ϕ_ϵ. We can assume all entries of M_ϵ are in $\mathcal{O}_{K'}$, the ring of integers of K'.

By bounding the number of points on the reduction of J_ϵ, using the same argument in Section 4.4.2, we know that we can take $S_2 = \{$places of bad reduction for $\mathcal{C}\} \cup \{$places dividing $2\} \cup \{$infinite places$\} \cup \{$places dividing $a\} \cup \{$places that divide$N_{K'/K}(\det M_\epsilon)\} \cup \{$places dividing all the coefficients of l_1 or $l_2\} \cup \{$places above primes less than $N'\}$. Here N' is a natural number such that any $x > N'$, we have $(x-1-4\sqrt{x})(x-3-4\sqrt{x})/2 > 64(x+1)$. In fact, we can take $N' = 300$. Note, as in Remark 4.4.6, we require f to be defined over $\mathcal{O}_K$ and all entries of M_ϵ in $\mathcal{O}_{K'}$.

Remark 5.4.1. We make the same three remarks as in Remark 4.4.7 on some practical issues.

5.5 Algorithm and Worked Example

In this section, we describe an algorithm for computing $\langle \epsilon, \eta \rangle_{CT}$ for $\epsilon, \eta \in \mathrm{Sel}^2(J)$ using the formula in Theorem 5.1.1. Recall, we assume the twisted Kummer surface $\mathcal{K}_\eta$ has a K-rational point. We also present a worked example that shows the improvement of the rank bound using the Cassels-Tate pairing.

5.5.1 Description of the algorithm

In this section, we describe an algorithm for computing the Cassels-Tate pairing $\langle \epsilon, \eta \rangle_{CT}$ for $\epsilon, \eta \in \mathrm{Sel}^2(J)$, using the formula in Theorem 5.1.1. Here we assume that the twisted Kummer surface $\mathcal{K}_\eta$ has a K-rational point. Note that this algorithm in theory works over any number field but we only computed examples in the case $K = \mathbb{Q}$.

We start with a genus two curve $\mathcal{C}$ with the following defining equation which we can assume to be defined over $\mathcal{O}_K$ by rescaling y:

$$\mathcal{C} : y^2 = f(x) = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0.$$

- Step 1: For $\epsilon, \eta \in \mathrm{Sel}^2(J)$, compute their representations $(\delta_1, n_1), (\delta_2, n_2)$, where $\delta_1, \delta_2 \in L^*$, $n_1^2 = N(\delta_1), n_2^2 = N(\delta_2)$ with $L = K[x]/(f)$ as in Remark 1.10.6. Recall Remark 3.2.8 for computing δ_1, δ_2 and we assume $\mathcal{K}_\eta$ has a K-rational point.

- Step 2: Apply the naive method described in Section 3.2 to compute the linear isomorphism $\psi_\eta : \mathcal{K}_\eta \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ which is represented by a matrix N_η.

- Step 3: Compute G_η, the defining equation for $\mathcal{K}_\eta$ using ψ_η from Step 2. Then search for a K-rational point R on $\mathcal{K}_\eta$ using the PointSearch function in MAGMA.

- Step 4: Compute the linear isomorphism $J_\eta \subset \mathbb{P}^{15} \xrightarrow{\phi_\eta} J \subset \mathbb{P}^{15}$ given in Theorem 1.11.1. Note, here we potentially need to replace ψ_η by the linear map represented by $M_T N_\eta$ for some $T \in J[2]$ such that $(\sigma \mapsto \phi_\eta(\phi_\eta^{-1})^\sigma), (\sigma \mapsto \psi_\eta(\psi_\eta^{-1})^\sigma)$ give the same cocycle for η. Explicit formula for M_T for $T \in J[2]$ is in Lemma 3.2.1.

- Step 5: Compute nonzero $a \in K$ such that the field of definition of the preimages of R in J_η is $K(\sqrt{a})$ via Remark 5.2.13.

The rest of the algorithm is under the assumption that $K(\sqrt{a}) \neq K$. Else, $\langle \epsilon, \eta \rangle_{CT}$ is trivial for any $\epsilon \in \mathrm{Sel}^2(J)$ as discussed in Remark 5.1.8.

- Step 6: Compute the isomorphisms $\phi_\epsilon, \psi_\epsilon$ and the defining equation G_ϵ for $\mathcal{K}_\epsilon$ similarly as above.

- Step 7: Compute $\psi_{\epsilon+\eta}$ similarly. Suppose $\psi_\epsilon(\psi_\epsilon^{-1})^\sigma, \psi_\eta(\psi_\eta^{-1})^\sigma$ represent the action of translation by $\epsilon_\sigma, \eta_\sigma$. We require $\psi_{\epsilon+\eta}(\psi_{\epsilon+\eta}^{-1})^\sigma$ to represent the action of translation by $\epsilon_\sigma + \eta_\sigma$. This implies that the computed $\psi_{\epsilon+\eta}$ potentially differs from the one we want by composition of M_T for some $T \in J[2]$. Recall M_T represents the translation by $T \in J[2]$ on $\mathcal{K}$ and we have explicit formulae for them as in Lemma 3.2.1.

- Step 8: Compute the $(2,2,2)$-form $\mathcal{F}$ as constructed in Lemma 5.2.1. Then compute $\mathcal{F}_{\epsilon,\eta}$ via the linear isomorphisms $\psi_\epsilon, \psi_\epsilon$ and $\psi_{\epsilon+\eta}$ as defined in Section 5.2.2.

- Step 9: Compute the K-rational function g on J_ϵ with formula stated in Corollary 5.2.11 via the method explained at the end of Section 5.2.3.

- Step 10: Compute the bound $N_{\epsilon,\eta} \in \mathbb{N}$ such that any finite place v of K above any prime bigger than $N_{\epsilon,\eta}$, the local Cassels-Tate pairing between ϵ and η using the formula in Theorem 5.1.1 is trivial. This is explained in detail in Section 5.4.

- Step 11: For any place v of K that is above a prime less than the number $N_{\epsilon,\eta}$ computed in Step 10, find a local point P_v on J_ϵ avoiding the zeros and poles of the rational function g computed in Step 9.

- Step 12: Compute $\langle \epsilon, \eta \rangle_{CT}$ via the formula in Theorem 5.1.1.

Remark 5.5.1.

(i) In practice, we probably would not know whether or not $\mathcal{K}_\eta$ has a K-rational point before running the first 3 steps in the above algorithm. So we only proceed to the later steps if the point search on $\mathcal{K}_\eta$ is successful.

(ii) For the cocycle condition in Step 7, instead of checking the cocycle condition for all 16 choices, we only need to check those such that $\mathcal{F}_{\epsilon,\eta}$ is defined over K by Proposition 5.2.4. In particular, there is no need to check any cocycle if there is only one $T \in J[2]$ such that the twisted $(2,2,2)$-form corresponding to $M_T \circ \psi_{\epsilon+\eta}$ is defined over K.

(iii) Recall, from Corollary 5.2.11, we know g on J_ϵ is defined as the pull back of a rational function on $\mathcal{K}_\epsilon$. In practice, we need not pull back this rational function to J_ϵ. Instead, we just evaluate it on a local point on $\mathcal{K}_\epsilon$ avoiding the zeros and poles. Note we require that the local point on $\mathcal{K}_\epsilon$ does lift to a local point on J_ϵ, which we can check via Remark 5.2.13.

5.5.2 Worked example

Now we demonstrate the algorithm described in Section 5.5.1 with an example. In particular, we will see with this example, that computing the Cassels-Tate pairing on $\text{Sel}^2(J)$ does improve the rank bound obtained via a 2-descent.

We consider the genus two curve

$$\mathcal{C} : y^2 = f(x) = 2(x+1)(x-5)(x^4+1),$$

and define $L = \mathbb{Q}[x]/(f)$.

Note that here f has a rational root, which implies that each Selmer element is represented by its image in $L^*/(L^*)^2\mathbb{Q}^*$ by Remark 1.10.6.

- We pick $\epsilon, \eta \in \mathrm{Sel}^2(J)$ such that the image of ϵ in $L^*/(L^*)^2\mathbb{Q}^*$ is represented by $-52/313x^5+261/313x^4-52/313x+574/313$ and the image of η in $L^*/(L^*)^2\mathbb{Q}^*$ is represented by $-42/313x^5+271/313x^4-x^3+271/313x-42/313$, as given by MAGMA.

- We compute the defining equation G_η for $\mathcal{K}_\eta$ as below

$$\begin{aligned}G_\eta = {} & 709888x_1^4 - 5387552x_1^3x_2 - 2782048x_1^3x_3 - 2113024x_1^3x_4 \\ & + 15330400x_1^2x_2^2 + 15841504x_1^2x_2x_3 + 12025232x_1^2x_2x_4 + 4105600x_1^2x_3^2 \\ & + 6212560x_1^2x_3x_4 + 2358192x_1^2x_4^2 - 19384936x_1x_2^3 - 30063832x_1x_2^2x_3 \\ & - 22808272x_1x_2^2x_4 - 15593112x_1x_2x_3^2 - 23579968x_1x_2x_3x_4 \\ & - 8945504x_1x_2x_4^2 - 2706408x_1x_3^3 - 6114416x_1x_3^2x_4 - 4623680x_1x_3x_4^2 \\ & - 1169504x_1x_4^3 + 9190529x_2^4 + 19015676x_2^3x_3 + 14417956x_2^3x_4 \\ & + 14803982x_2^2x_3^2 + 22371548x_2^2x_3x_4 + 8482108x_2^2x_4^2 + 5142732x_2x_3^3 \\ & + 11609724x_2x_3^2x_4 + 8773336x_2x_3x_4^2 + 2217824x_2x_4^3 + 673081x_3^4 \\ & + 2016260x_3^3x_4 + 2276204x_3^2x_4^2 + 1146880x_3x_4^3 + 217464x_4^4.\end{aligned}$$

We get a rational point $R = (3 : 0 : 0 : 4)$ on $\mathcal{K}_\eta$ and $a = -1$ where the field of definition of the preimages of R in J_η is $\mathbb{Q}(\sqrt{a})$.

- We compute the defining equation G_ϵ for $\mathcal{K}_\epsilon$ as below

$$\begin{aligned}G_\epsilon = {} & 303804780x_1^4 + 331641136x_1^3x_2 + 346185336x_1^3x_3 + 125445776x_1^3x_4 \\ & + 135762832x_1^2x_2^2 + 283454352x_1^2x_2x_3 + 102705200x_1^2x_2x_4 \\ & + 147949648x_1^2x_3^2 + 107210504x_1^2x_3x_4 + 19428376x_1^2x_4^2 + 24701248x_1x_2^3 \\ & + 77364896x_1x_2^2x_3 + 28029408x_1x_2^2x_4 + 80767464x_1x_2x_3^2 \\ & + 58522240x_1x_2x_3x_4 + 10604336x_1x_2x_4^2 + 28105796x_1x_3^3 \\ & + 30546128x_1x_3^2x_4 + 11069656x_1x_3x_4^2 + 1337584x_1x_4^3 + 1685376x_2^4 \\ & + 7038688x_2^3x_3 + 2549888x_2^3x_4 + 11023176x_2^2x_3^2 + 7986400x_2^2x_3x_4 \\ & + 1447024x_2^2x_4^2 + 7672336x_2x_3^3 + 8337736x_2x_3^2x_4 + 3021264x_2x_3x_4^2 \\ & + 365040x_2x_4^3 + 2002477x_3^4 + 2901428x_3^3x_4 + 1576992x_3^2x_4^2 \\ & + 381064x_3x_4^3 + 34540x_4^4\end{aligned}$$

We compute the rational function g with formula stated in Corollary 5.2.11 and $(c_1, c_2, c_3, c_4) = (1, 0, 0, 0)$, viewed as a rational function on $\mathcal{K}_\epsilon$:

$$g = (-867472x_1^2 - 474752x_1x_2 - 488896x_1x_3 - 177632x_1x_4 - 64952x_2^2 \\ - 133780x_2x_3 - 48600x_2x_4 - 68881x_3^2 - 50064x_3x_4 - 9092x_4^2)/x_1^2.$$

- We include some local Cassels-Tate pairing computations. For a place v, we represent a local point on $\mathcal{K}_\epsilon(\mathbb{Q}_v)$ such that the first three coordinates are exact and we give enough precision or decimal places for the last coordinate to pin down a unique point on $\mathcal{K}_\epsilon(\mathbb{Q}_v)$. For a place v, we represent $g(P_v), a$ as elements in $\mathbb{Q}_v^*/(\mathbb{Q}_v^*)^2$.

places v	local points P_v on $\mathcal{K}_\epsilon$	$g(P_v)$	a	$(g(P_v), a)_v$
2	$(31 : 1 : 18 : 5 + O(2^3))$	-1	-1	-1
3	$(17/9 : 14 : 26 : 1/3 + O(3^0))$	-1	-1	1
313	$(159 \cdot 313^2 : 240 : 170 : 189 + O(313))$	1	-1	1
∞	$(6 : -15 : -4 : -7.70...)$	1	-1	1

- Following the discussion at the end of Section 5.4 and Remark 4.4.7, we have the following primes that potentially contribute to $\langle \epsilon, \eta \rangle_{CT}$:
  - Prime 2;
  - Primes of bad reduction of the genus two curve $\mathcal{C}$: 2, 3, 313;
  - Primes arise from M_ϵ, denoted by S' in Remark 4.4.7(ii): 2, 3, 5, 19, 31, 113, 313;
  - Primes below 300.

  It turns out that the only place where the local Cassels-Tate pairing between ϵ and η is nontrivial is 2 and so $\langle \epsilon, \eta \rangle_{CT} = -1$.

Remark 5.5.2.

(i) As discussed in Remark 4.4.7, we probably have computed the local Cassels-Tate pairing for more primes than needed. We also suspect that via some suitable minimization and reduction techniques, we can simplify the set of primes that potentially contribute to $\langle \epsilon, \eta \rangle_{CT}$. However, this does not have much effect on the computation as the local Cassels-Tate paring is fast to compute, even for very large primes.

(ii) We list a few sanity checks throughout the computation. We verified that all the defining equations of the twisted Kummer surfaces and the twisted

$(2,2,2)$ forms are indeed defined over $\mathbb{Q}$. For each local Cassels-Tate pairing computations, we computed 100 local points at random and verified that these local points all give the same value of the local pairing.

Note that in this example, $|\mathrm{Sel}^2(J)| = 2^3$ and $|J(\mathbb{Q})[2]| = 2^1$ which implies that $|\ker\langle\ ,\ \rangle_{CT}| \geq 2^1$. On the other hand, we note that $\mathcal{C}$ has a rational point $(-1,0)$. This implies the Cassels-Tate pairing on $\mathrm{Sel}^2(J) \times \mathrm{Sel}^2(J)$ is in fact alternating by Lemma 1.8.3. Since $\langle \epsilon, \eta \rangle_{CT} = -1$, we get $|\ker\langle\ ,\ \rangle_{CT}| \leq 2^1$. Therefore, we deduce that $|\ker\langle\ ,\ \rangle_{CT}| = 2^1$.

Recall in Remark 1.9.4(i), we showed that we can potentially improve the rank bound from a descent calculation via computing the Cassels-Tate pairing as $J(K)/2(J(K)) \subset \ker\langle\ ,\ \rangle_{CT} \subset \mathrm{Sel}^2(J)$. This is indeed true and in this example, we improve the rank bound from $2^r \leq |\mathrm{Sel}^2(J)|/|J(K)[2]| = 2^2$ to $2^r \leq |\ker\langle\ ,\ \rangle_{CT}|/|J(K)[2]| = 2^0$. Therefore, we not only improved the rank bound but also proved that the rank of this particular Jacobian variety is in fact equal to 0.

Chapter 6

Improving the Algorithm Using the Flex Algebra

Throughout this chapter, we let J denote the Jacobian variety of a genus two curve $\mathcal{C}$ defined by $y^2 = f(x)$ where f is a degree 6 polynomial with coefficients in K and $\triangle(f) \neq 0$. In Section 5.5.1, we described an algorithm for computing the Cassels-Tate pairing on $\text{Sel}^2(J) \times \text{Sel}^2(J)$. More explicitly, for $\epsilon, \eta \in \text{Sel}^2(J)$, we computed $\langle \epsilon, \eta \rangle_{CT}$ using the formula in Theorem 5.1.1 and Corollary 5.2.11. Recall that we need to be under the assumption that the twisted Kummer $\mathcal{K}_\eta$ has a K-rational point. In the original algorithm, we used the naive method described in Section 3.2 to compute $\psi_\epsilon : \mathcal{K}_\epsilon \to \mathcal{K}$ corresponding to ϵ and used the explicit isomorphism given in Theorem 1.11.1 to compute $\phi_\epsilon : J_\epsilon \to J$, where $(J_\epsilon, [2] \circ \phi_\epsilon)$ is the 2-covering of J corresponding to ϵ. Recall such ψ_ϵ are precisely the linear isomorphisms $\mathcal{K}_\epsilon \to \mathcal{K}$ that preserve the action of $J[2]$, as shown in Lemma 3.2.2. By the field of definition of the formula for ϕ_ϵ given in Theorem 1.11.1 and the naive method described in Section 3.2, the explicit computation related to ϵ for the Cassels-Tate pairing was done over $L_2 = L_1(\sqrt{a_1}, ..., \sqrt{a_6})$. Here L_1 denotes the splitting field of $f(x)$ and $(a_1, ..., a_6)$ represents the image of ϵ in $L^*/(L^*)^2K^*$ under the natural isomorphism $\bar{L} \cong \bar{K}^6$ with $L = K[x]/(f)$, as described in Section 1.10.1. In this chapter, we will improve this algorithm by using the flex algebra method described in Section 3.3, in the general case. The advantage of this method is that we will be working over a smaller number field. Note that in Section 6.2.1, we will give a precise definition of what we mean by the general case.

6.1 Twist of the Desingularized Kummer Surface

Recall in Sections 1.2.5 and 1.3.4, we denote the desingularized Kummer surface by $\mathcal{S}$ and its embedding in $\mathbb{P}^5$ is defined to be the locus of $(p_0 : ... : p_5)$ for which $P(x)^2$ is congruent to a quadratic in x modulo $f(x)$, where $P(x) = \sum_{j=0}^{5} p_j x^j$. We also showed that the projection of $J \subset \mathbb{P}^{15}_{\{k_{ij}, b_i\}} \to \mathbb{P}^5$ onto the 6 odd coordinates $b_1, ..., b_6$ is isomorphic to $\mathcal{S}$ with the explicit linear isomorphism given in Proposition 1.3.8. In this section, we study the twist of $\mathcal{S}$ corresponding to an element in $\text{Sel}^2(J)$.

Remark 6.1.1. We know that points of $J[2]$ act on $\mathcal{K}$ by translation. Since $\mathcal{S}$ is the desingularization of $\mathcal{K}$ and the action of $J[2]$ preserves the set of singular points on $\mathcal{K}$, translation by points of $J[2]$ on $\mathcal{S}$ is defined to be the unique extension of the translation by points of $J[2]$ on $\mathcal{K}$. In particular, we have the commutative diagram:

$$\begin{array}{ccc} \mathcal{S} & \longrightarrow & \mathcal{S} \\ {\scriptstyle blow-up}\downarrow & & \downarrow{\scriptstyle blow-up} \\ \mathcal{K} & \xrightarrow{M_P} & \mathcal{K}, \end{array}$$

where M_P represents the translation of $P \in J[2]$ on $\mathcal{K}$ and the blow-up morphism $\mathcal{S} \to \mathcal{K}$ has explicit formula given in Remark 1.3.9. The unique morphism $\mathcal{S} \to \mathcal{S}$ that makes this diagram commute is the action of τ_P on $\mathcal{S}$.

6.1.1 Twisted desingularized Kummer

Fix $\epsilon \in \mathrm{Sel}^2(J)$ for the Jacobian variety J of $\mathcal{C}$. We say $\mathcal{S}_\epsilon$ is the twist of $\mathcal{S}$ corresponding to ϵ if $\mathcal{S}_\epsilon$ is a variety defined over K and there exists an isomorphism $\Psi : \mathcal{S}_\epsilon \to \mathcal{S}$ defined over $\bar{K}$ such that $\Psi(\Psi^{-1})^\sigma$ is the action of $\epsilon_\sigma \in J[2]$ on $\mathcal{S}$ and $(\sigma \mapsto \epsilon_\sigma)$ is a cocycle representing ϵ.

We now follow [FTvL12, Chapter 4] and give an explicit description of the twisted desingularized Kummer surface $\mathcal{S}_\epsilon$ corresponding to ϵ. It is also the desingularization of the twisted Kummer $\mathcal{K}_\epsilon$ as discussed at the end of Chapter 7 of [FTvL12].

Suppose the image of ϵ in $L^*/(L^*)^2K^*$ is represented by $\delta \in L^*$ as described in Section 1.10.1. Then the embedding of $\mathcal{S}_\epsilon$ in $\mathbb{P}^5$ is defined to be the locus of $(p_0 : \ldots : p_5)$ for which $\delta P(x)^2$ is congruent to a quadratic in x modulo $f(x)$ where $P(x) = \sum_{j=0}^{5} p_j x^j$.

6.1.2 Explicit twist map of the desingularized Kummer

Let $(J_\epsilon, [2]\circ\phi_\epsilon)$ denote the 2-covering of J corresponding to $\epsilon \in \mathrm{Sel}^2(J)$ for some isomorphism $\phi_\epsilon : J_\epsilon \to J$. By the definitions of $\mathcal{S}$ and its twist $\mathcal{S}_\epsilon$ embedded in $\mathbb{P}^5$, we quote the following natural twist map corresponding to ϵ as described in [FTvL12, Proposition 4.1, Corollary 4.2].

Lemma 6.1.2. *Suppose $\epsilon \in Sel^2(J)$ is represented by (δ, n) as in Remark 1.10.6, where $\delta \in L^*$ represents the image of ϵ in $L^*/(L^*)^2K^*$. Let $\zeta \in \bar{L}^*$ satisfy $\zeta^2 = \delta$ and $N(\zeta) = n$. Then we have the following linear isomorphism corresponding to the twist by ϵ:*

$$\mathcal{S}_\epsilon \subset \mathbb{P}^5 \to \mathcal{S} \subset \mathbb{P}^5,$$

that sends $(p_0 : ... : p_5) \mapsto (p'_0 : ... : p'_5)$ *where* $\zeta \cdot \sum_{j=0}^5 p_j x^j = \sum_{j=0}^5 p'_j x^j \in \bar{L}$.

Remark 6.1.3. In this remark, we give more details to the explicit construction of the linear isomorphism $\phi_\epsilon : J_\epsilon \subset \mathbb{P}^{15}_{\{u_i,v_i\}} \to J \subset \mathbb{P}^{15}_{\{k_{ij},b_i\}}$ corresponding to ϵ described in Theorem 1.11.1 and Remark 1.11.2. Recall that ϕ_ϵ is represented by $\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}$ with some $A \in \mathrm{GL}_{10}(\bar{K})$ and $B \in \mathrm{GL}_6(\bar{K})$. In fact, following the proof in [FTvL12], the matrix B, under the change of basis described in Proposition 1.3.8, precisely represents the multiplication by $\zeta \in \bar{L}$ as constructed in Lemma 6.1.2, for the ζ that is in the construction for ϕ_ϵ.

6.2 Computation over the Flex Algebra

In this section, we fix $\epsilon \in \mathrm{Sel}^2(J)$ and $(J_\epsilon, [2] \circ \phi_\epsilon)$ the 2-covering of J corresponding to ϵ for some isomorphism $\phi_\epsilon : J_\epsilon \to J$. In particular, Theorem 1.11.1 constructs such isomorphism where we embed J_ϵ in $\mathbb{P}^{15}$ with a set of Galois invariant coordinates $u_0, ..., u_9, v_1, ..., v_6$ and embed J in $\mathbb{P}^{15}$ with the standard coordinates $k_{11}, k_{12}, .., k_{44}, b_1, ..., b_6$. Moreover, by Remark 1.11.2, we know such $\phi_\epsilon : J_\epsilon \subset \mathbb{P}^{15}_{\{u_i,v_i\}} \to J \subset \mathbb{P}^{15}_{\{k_{ij},b_i\}}$ is represented by $\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}$ with some $A \in \mathrm{GL}_{10}(\bar{K})$ and $B \in \mathrm{GL}_6(\bar{K})$. We will describe a method for computing the isomorphism ϕ_ϵ over a field that is smaller than what is required in the method for computing ϕ_ϵ via the explicit formula in Theorem 1.11.1. Here, we require that the action of the Galois group G_K on the corresponding $J[2]$-torsor is general and we make this assumption precise in Section 6.2.1.

6.2.1 Galois action on $J[2]$-torsors

Recall in Section 1.7.2, we described the Galois action on $J[2]$ using symplectic group $\mathrm{Sp}_4(\mathbb{F}_2)$ and viewing $J[2]$ as a $\mathbb{F}_2$-vector space of dimension 4. In Lemma 1.7.7(i), we showed $\mathrm{Sp}_4(\mathbb{F}_2) \cong S_6$. In this section, we study the Galois action on $\phi_\epsilon^{-1}(J[2])$, using the *affine symplectic group* $\mathrm{ASp}_4(\mathbb{F}_2)$, which is defined as

$$\mathrm{ASp}_4(\mathbb{F}_2) = \{\mathbb{F}_2^4 \xrightarrow{f} \mathbb{F}_2^4 : f(x) = Ax + b \text{ for some } A \in \mathrm{Sp}_4(\mathbb{F}_2), b \in \mathbb{F}_2^4\},$$

and we have a natural short exact sequence

$$0 \to \mathbb{F}_2^4 \to \mathrm{ASp}_4(\mathbb{F}_2) \to \mathrm{Sp}_4(\mathbb{F}_2) \to 0. \tag{6.2.1}$$

As explained in Remark 3.3.11, $\phi_\epsilon^{-1}(J[2])$ is a $J[2]$-torsor corresponding to $\epsilon \in \mathrm{Sel}^2(J)$, which is a zero-dimensional variety defined over K. Hence, $\sigma \in G_K$ induces an automorphism of it. Via the isomorphism $\phi_\epsilon : J_\epsilon \to J$, this induces

an automorphism of $J[2]$ that is $\phi_\epsilon \circ \sigma \circ \phi_\epsilon^{-1} = \tau_{\epsilon_\sigma} \circ \sigma$, where $\phi_\epsilon(\phi_\epsilon^{-1})^\sigma = \tau_{\epsilon_\sigma}$ and $(\sigma \mapsto \epsilon_\sigma)$ is a cocycle representation for ϵ. This implies the action of G_K on $\phi_\epsilon^{-1}(J[2])$ corresponds to elements in $\mathrm{ASp}_4(\mathbb{F}_2)$. In particular, this induces a group homomorphism $G_K \xrightarrow{\nu} \mathrm{ASp}_4(\mathbb{F}_2)$ as $\tau(\sigma(P) + \epsilon_\sigma) + \epsilon_\tau = \tau\sigma(P) + \epsilon_{\tau\sigma}$ for every $P \in J[2]$, $\sigma, \tau \in G_K$. Let M denote the smallest field over which all points in $\phi_\epsilon^{-1}(J[2])$ are defined. We know $\ker \nu = G_M$ and hence ν induces an injective group homomorphism $G_{M/K} \to \mathrm{ASp}_4(\mathbb{F}_2)$. We have the following proposition.

Proposition 6.2.1. *$G_K \xrightarrow{\nu} ASp_4(\mathbb{F}_2)$ is surjective if and only if*

(i) $Gal(f) = S_6$;

(ii) $K(P)$ is a degree 16 extension of K for any $P \in \phi_\epsilon^{-1}(J[2])$.

Proof. Suppose ν is surjective. By the short exact sequence (6.2.1), we know $G_K \to \mathrm{Sp}_4(\mathbb{F}_2)$ is surjective. Hence, by Lemma 1.7.7(ii), we know (i) holds. Since the action of G_K is transitive on $\phi_\epsilon^{-1}(J[2])$, we get (ii).

Suppose (i) (ii) both hold and $P \in \phi_\epsilon^{-1}(J[2])$. By potentially composing ϕ_ϵ with a translation by a two-torsion point on J, we can assume $\phi_\epsilon(P) = \mathcal{O}_J$. The action of $G_{M/K}$ on $\phi_\epsilon^{-1}(J[2])$ has one orbit and $\mathrm{Stab}_{G_{M/K}}(P) \cong \mathrm{Sp}_4(\mathbb{F}_2)$. Hence, by the orbit-stabilizer theorem, we have $|G_{M/K}| = |\mathrm{ASp}_4(\mathbb{F}_2)|$. Since $G_{M/K} \cong \mathrm{Im}\,\nu$, we get ν is surjective as required.

□

Remark 6.2.2. Suppose ν is surjective. Then $G_{M/K} \cong \mathrm{Im}\,\nu = \mathrm{ASp}_4(\mathbb{F}_2)$ by the first isomorphism theorem. Recall we denote the splitting field of f by L_1 and G_{L_1} is the kernel of $G_K \to \mathrm{Sp}_4(\mathbb{F}_2)$ induced by the action of G_K on $J[2]$. This implies, by the exact sequence (6.2.1) and $\ker \nu = G_M$, that $G_M \subset G_{L_1}$ and so L_1 is a sub-extension of M. By the tower law of field extensions and Proposition 6.2.1(i), we get $|G_{M/L_1}| = 16$. Since any $\sigma \in G_{M/L_1}$ acts trivially on $J[2]$, ν induces a group homomorphism $G_{M/L_1} \to \mathrm{ASp}_4(\mathbb{F}_2)$:

$$\sigma \mapsto \tau_{\epsilon_\sigma}.$$

Since the above map is injective, a size count shows that the map $\sigma \in G_{M/L_1} \mapsto \epsilon_\sigma$ is sujective on $J[2]$. This implies that all points in $\phi_\epsilon^{-1}(J[2])$ are in fact conjugate to each other over L_1. Moreover, via the above discussion we can interpret the exact sequence (6.2.1) as

$$0 \to G_{M/L_1} \to G_{M/K} \to G_{L_1/K} \to 0.$$

In the following proposition, we prove more results under the assumption that $G_K \xrightarrow{\nu} \mathrm{ASp}_4(\mathbb{F}_2)$ is surjective.

Proposition 6.2.3. *Suppose $G_K \xrightarrow{\nu} ASp_4(\mathbb{F}_2)$ is surjective. Suppose $P \in \phi_\epsilon^{-1}(J[2])$. Then we have the following.*

(i) P is the unique point in $\phi_\epsilon^{-1}(J[2])$ that is defined over $K(P)$.

(ii) There is no field F_0 such that $K \subsetneq F_0 \subsetneq K(P)$.

Proof. Note by potentially composing ϕ_ϵ with a translation by a two-torsion point on J, we can assume $\phi_\epsilon(P) = \mathcal{O}_J$. We know $G_{M/K} \cong \operatorname{Im}\nu = \mathrm{ASp}_4(\mathbb{F}_2)$. Consider the action of $G_{M/K}$ on $\phi_\epsilon^{-1}(J[2])$. We know $G_{M/K(P)} = \mathrm{Stab}_{G_{M/K}} P$. Since $\phi_\epsilon(P) = \mathcal{O}_J$ which is defined over K, the induced action of $G_{M/K(P)}$ on $J[2]$ gives $\mathrm{Sp}_4(\mathbb{F}_2)$. But the only fixed point of $\mathrm{Sp}_4(\mathbb{F}_2)$ is 0 as $\mathrm{Sp}_4(\mathbb{F}_2)$ acts transitively on $\mathbb{F}_2^4 \setminus \{0\}$, which gives (i).

Suppose there exists F_0 such that $K \subsetneq F_0 \subsetneq K(P)$. Then $\mathrm{Gal}_{M/K(P)} \cong \mathrm{Sp}_4(\mathbb{F}_2) \subsetneq \mathrm{Gal}_{M/F_0} \subsetneq \mathrm{Gal}_{M/K} \cong \mathrm{ASp}_4(\mathbb{F}_2)$. However, we observe that $\mathrm{Sp}_4(\mathbb{F}_2)$ is a maximal subgroup in $\mathrm{ASp}_4(\mathbb{F}_2)$. This is because suppose we have $\mathrm{Sp}_4(\mathbb{F}_2) \subsetneq H \subset \mathrm{ASp}_4(\mathbb{F}_2)$, then $H \cap \mathbb{F}_2^4 \neq 0$ which implies $\mathbb{F}_2^4 \subset H$ as $\mathrm{Sp}_4(\mathbb{F}_2)$ acts transitively on $\mathbb{F}_2^4 \setminus \{0\}$, and therefore $H = \mathrm{ASp}_4(\mathbb{F}_2)$. Hence, we have a contradiction which proves (ii).

□

For $\epsilon \in \mathrm{Sel}^2(J)$, we say we are in the *general case* when the corresponding homomorphism $G_K \xrightarrow{\nu} \mathrm{ASp}_4(\mathbb{F}_2)$ defined at the start of this section is surjective. From now on, we always assume we are in this case and therefore we have the statements (i) and (ii) in Proposition 6.2.3. Note that we make this assumption so that the étale algebras considered below are always fields. This simplifies some of the arguments.

6.2.2 Twist of J over the flex algebra

Let F denote the flex algebra of ϵ as defined in Definition 3.3.12. We view F as the étale algebra $\mathrm{Map}_K(\phi_\epsilon^{-1}(J[2]), \bar{K})$ by Lemma 3.3.13. By Proposition 6.2.1(ii), we know that F is isomorphic to an extension of K of degree 16 and we fix an embedding of F in $\bar{K}$. This implies that $F = K(P)$ for some $P \in \phi_\epsilon^{-1}(J[2])$. Recall the flex algebra method in Section 3.3 gives a linear isomorphism $\psi_\epsilon : \mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ corresponding to ϵ and defined over F. Now fix $\mathcal{K}_\epsilon$ as a subvariety in $\mathbb{P}^3$. By Lemma 3.2.2, we know that there are precisely 16 choices of linear isomorphisms $\mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ that correspond to ϵ, namely $M_P \circ \psi_\epsilon$ for $P \in J[2]$. Note here M_P represents the the action of translation by P on $\mathcal{K}$. By the assumption $\mathrm{Gal}(f) = S_6$, we know the 16 linear isomorphisms $\mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ corresponding to ϵ give rise to the 16 different cocycles for ϵ. On the other hand, we know the 16 singular points on $\mathcal{K}_\epsilon$ are Galois conjugates over L_1, the splitting field of f, as discussed in Remark 6.2.2. Hence, there exists $\sigma_1, ..., \sigma_{16} \in G_{L_1}$ such that $\sigma_1(\psi_\epsilon), ..., \sigma_{16}(\psi_\epsilon)$ are the 16 different linear isomorphisms $\mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ corresponding to ϵ, each

is defined over $\sigma_i(F)$ and gives a different cocycle for ϵ. Since ϵ is not trivial, $\sigma_i(F)$ is in fact the field of definition of $\sigma_i(\psi_\epsilon)$ by Proposition 6.2.3(ii). Recall, we assume we are in the general case.

Suppose ϵ is represented by (δ, n) with $\delta \in L^*$ representing the image of ϵ in $L^*/(L^*)^2K^*$ and $N(\delta) = n^2$ as in Remark 1.10.6. In this section, we will describe a method that computes a linear isomorphism $\phi_\epsilon : J_\epsilon \subset \mathbb{P}^{15} \to J \subset \mathbb{P}^{15}$ corresponding to ϵ over F, in the general case. We will need to show that there exists a computable linear isomorphism $\mathcal{S}_\epsilon \subset \mathbb{P}^5 \to \mathcal{S} \subset \mathbb{P}^5$ corresponding to ϵ that is defined over F and constructed as in Lemma 6.1.2. Since there exists an element in $\phi_\epsilon^{-1}(J[2])$ defined over F, we know ϵ is trivial in $H^1(G_F, J[2])$ and so $\delta \in (L_F^*)^2F^*$ where $L_F = L \otimes F = F[x]/(f)$. This implies that there exist $\lambda \in F^*, \beta \in L_F^*$ such that $\lambda\beta^2 = \delta$. We note the multiplication by β gives the same morphism $\mathcal{S}_\epsilon \subset \mathbb{P}^5 \to \mathcal{S} \subset \mathbb{P}^5$ as the multiplication by $\sqrt{\lambda}\beta$. More work needs to be done in order to further satisfy the condition $N(\sqrt{\lambda}\beta) = n$ as required by Lemma 6.1.2.

First, recall the explicit construction of the twist described in Theorem 1.11.1 and Remark 1.11.2. We note the following choices made in the construction. We need to pick $\zeta \in \bar{L}$ satisfying $\zeta^2 = \delta$ with $N(\zeta) = n$. Observe the extra condition that the diagonal entries of T_1, as defined in Remark 1.11.2, are nonzero is automatically satisfied as we are in the general case. We now prove the following properties of the linear isomorphisms constructed as in Theorem 1.11.1 and Remark 1.11.2.

Note that in this section, by Hilbert's Theorem 90, any matrix representation for a linear morphism between projective spaces is assumed to be defined over the field of definition of the morphism, unless stated otherwise.

Proposition 6.2.4. *Under the assumptions in this section, the following statements hold:*

(i) Suppose $\phi_\epsilon : J_\epsilon \subset \mathbb{P}^{15} \to J \subset \mathbb{P}^{15}$ is an isomorphism corresponding to ϵ and constructed as in Theorem 1.11.1, then $\sigma(\phi_\epsilon)$ is also an isomorphism corresponding to ϵ and constructed as in Theorem 1.11.1, for any $\sigma \in G_{L_1}$.

(ii) For any cocycle $(\sigma \mapsto \epsilon_\sigma)$ representing ϵ, there exists an isomorphism $\phi_\epsilon : J_\epsilon \subset \mathbb{P}^{15} \to J \subset \mathbb{P}^{15}$ corresponding to ϵ and constructed as in Theorem 1.11.1 such that $\phi_\epsilon(\phi_\epsilon^{-1})^\sigma = \tau_{\epsilon_\sigma}$.

(iii) Suppose an isomorphism $\phi_\epsilon : J_\epsilon \subset \mathbb{P}^{15} \to J \subset \mathbb{P}^{15}$ corresponding to ϵ is represented by a matrix in the form of $\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}$, with some $A \in GL_{10}(\bar{K})$ and $B \in GL_6(\bar{K})$. The field of definition of A is F if and only if the field of definition of B is F.

Proof. From the explicit construction described in Remark 1.11.2, it can be checked that the only effect of the action of $\sigma \in G_{L_1}$ is potentially the change of the value of $\zeta(\omega_i)$ to the other square root of $\delta(\omega_i)$ while keeping $\prod_{i=1}^{6} \zeta(\omega_i) = n$, where $\omega_1, ..., \omega_6$ are the roots of f. Hence, $\sigma(\phi_\epsilon) : J_\epsilon \subset \mathbb{P}^{15} \to J \subset \mathbb{P}^{15}$ is also an linear isomorphism corresponding to ϵ and constructed as in Theorem 1.11.1 which proves (i).

Let $\phi_\epsilon : J_\epsilon \subset \mathbb{P}^{15} \to J \subset \mathbb{P}^{15}$ be an isomorphism constructed as in Theorem 1.11.1 and $\phi_\epsilon(\phi_\epsilon^{-1})^\sigma = \tau_{\epsilon_\sigma}$ with $(\sigma \mapsto \epsilon_\sigma)$ a cocycle representing ϵ. Suppose $(\sigma \mapsto \epsilon'_\sigma)$ is another cocycle representing ϵ. By the argument at the start of Section 6.2.2, there exists $\psi_\epsilon : \mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ such that $\psi_\epsilon(\psi_\epsilon^{-1})^\sigma$ is the action of ϵ_σ on $\mathcal{K} \subset \mathbb{P}^3$ and there exists $\tau \in G_{L_1}$ such that $\tau(\psi_\epsilon)$ gives the cocycle $(\sigma \mapsto \epsilon'_\sigma)$. It can be checked that $\tau(\phi_\epsilon)$ also gives the cocycle $(\sigma \mapsto \epsilon'_\sigma)$ and it is indeed constructed as in Theorem 1.11.1 by (i). This proves (ii).

Lastly, there are only 16 choices of linear isomorphisms $J_\epsilon \subset \mathbb{P}^{15} \to J \subset \mathbb{P}^{15}$ corresponding to ϵ by Remark 1.5.9 which implies ϕ_ϵ is defined over a degree 16 extension of K. If the field of definition of A is a degree 16 extension F of K, then the field of definition of ϕ_ϵ is equal to F and so B is also defined over F. Since ϵ is not trivial and by assumption there is no nontrivial subfield of F, we know the field of definition of B is F. The same argument proves the other direction which then proves (iii)

□

We now show that there exists a computable linear isomorphism $\mathcal{S}_\epsilon \subset \mathbb{P}^5 \to \mathcal{S} \subset \mathbb{P}^5$ corresponding to ϵ that is defined over F and constructed as in Lemma 6.1.2.

Recall there exists $\psi_\epsilon : \mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ corresponding to ϵ with the field of definition being F. Suppose we have $\mathcal{K}$ and $\mathcal{K}_\epsilon$ both embedded in $\mathbb{P}^3$ with Galois invariant coordinates $k_1, ..., k_4$ and $k'_1, ..., k'_4$, respectively. Let $k_{ij} = k_i k_j$ and $k'_{ij} = k'_i k'_j$. We can also embed $\mathcal{K}, \mathcal{K}_\epsilon$ in $\mathbb{P}^9_{k_{ij}}$ and $\mathbb{P}^9_{k'_{ij}}$ respectively and let $A_\epsilon \in \mathrm{GL}_{10}(F)$ represent the linear map $\mathcal{K}_\epsilon \subset \mathbb{P}^9_{k'_{ij}} \to \mathcal{K} \subset \mathbb{P}^9_{k_{ij}}$ induced by ψ_ϵ. By Proposition 6.2.4(ii), there exits an isomorphism $\phi_\epsilon : J_\epsilon \subset \mathbb{P}^{15}_{\{u_i, v_i\}} \to J \subset \mathbb{P}^{15}_{\{k_{ij}, b_i\}}$ corresponding to ϵ constructed as in Theorem 1.11.1 and give the same cocycle as the one given by ψ_ϵ. Suppose it is represented by $M_\epsilon = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}$. By the following commutative diagram

$$\begin{array}{ccccc} J_\epsilon \subset \mathbb{P}^{15}_{\{u_i,v_i\}} & \xrightarrow{proj} & \mathbb{P}^9_{u_i} & \longrightarrow & \mathbb{P}^9_{k'_{ij}} \\ \downarrow{\scriptstyle \phi_\epsilon} & & \downarrow{\scriptstyle A} & \swarrow{\scriptstyle A_\epsilon} & \\ J \subset \mathbb{P}^{15}_{\{k_{ij},b_i\}} & \xrightarrow{proj} & \mathbb{P}^9_{k_{ij}} & & \end{array},$$

we deduce $A^{-1}A_\epsilon$ is defined over K. Hence, the field of definition of A is F and so the field of definition of B is also F by Proposition 6.2.4(iii). By Remark 6.1.3, we know that there exits $\zeta \in \bar{L}$ such that $N(\zeta) = n$, $\zeta^2 = \delta$ and the linear isomorphism $\mathcal{S}_\epsilon \subset \mathbb{P}^5 \to \mathcal{S} \subset \mathbb{P}^5$ induced by the multiplication by ζ is defined over F. Hence, let L_F denote $L \otimes F = F[x]/(f)$ and there exists $\beta \in L_F^*$ such that $\lambda\beta^2 = \delta$ for some $\lambda \in F$ and $N(\sqrt{\lambda}\beta) = n$. We note that $N(\sqrt{\lambda}\beta)$ is independent of the choice of square root of λ and the multiplication by ζ is the same isomorphism $\mathcal{S}_\epsilon \subset \mathbb{P}^5 \to \mathcal{S} \subset \mathbb{P}^5$ as the multiplication by β.

Suppose we have computed some $\beta \in L_F^*$ such that $\lambda\beta^2 = \delta$ for some $\lambda \in F$ and $N(\sqrt{\lambda}\beta) = n$. Let $B_\epsilon \in \mathrm{GL}_6(F)$ represent $\mathcal{S}_\epsilon \subset \mathbb{P}^5_{b'_i} \to \mathcal{S} \subset \mathbb{P}^5_{b_i}$ which is the composition of the linear isomorphism $\mathcal{S}_\epsilon \subset \mathbb{P}^5 \to \mathcal{S} \subset \mathbb{P}^5$ that is the multiplication by β which is defined over F corresponding to the twist by ϵ as described above, and the linear change of coordinates given in Proposition 1.3.8. Note here we let $b'_1, ..., b'_6$ denote the coordinates of the ambient space of $\mathcal{S}_\epsilon$ that are Galois invariant. We have the following proposition.

Proposition 6.2.5. *Embed J_ϵ in $\mathbb{P}^{15}$ with Galois invariant coordinates k'_{11}, k'_{12}, $..., k'_{44}, b'_1, ..., b'_6$. There exists a unique $t \in F$ such that the matrix*

$$M_\epsilon = \begin{bmatrix} A_\epsilon & 0 \\ 0 & tB_\epsilon \end{bmatrix}$$

represents a twist $J_\epsilon \subset \mathbb{P}^{15}_{\{k'_{ij}, b'_i\}} \to J \subset \mathbb{P}^{15}_{\{k_{ij}, b_i\}}$ that is corresponding to ϵ and defined over F.

Proof. By the definition of β in the construction of B_ϵ, we know there exists an isomorphism $\phi_\epsilon : J_\epsilon \subset \mathbb{P}^{15}_{\{u_i, v_i\}} \to J \subset \mathbb{P}^{15}_{\{k_{ij}, b_i\}}$ constructed by $\zeta = \sqrt{\lambda}\beta$ in Theorem 1.11.1. Hence, ϕ_ϵ is represented by $\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}$, with some $A \in \mathrm{GL}_{10}(\bar{K})$ and $B \in \mathrm{GL}_6(\bar{K})$. Moreover, via a change of coordinates between $b_1, ..., b_6$ and $v_1, ..., v_6$ over K given in Proposition 1.3.8, we have $B = B_\epsilon$ projectively. Since the field of definition of B_ϵ is F, the field of definition of A is also F by Proposition 6.2.4(iii). Hence, by the argument at the beginning of Section 6.2.2, $A_\epsilon(A_\epsilon^{-1})^\sigma = A(A^{-1})^\sigma$ for all $\sigma \in G_K$. Since both $k'_{11}, k'_{12}, ..., k'_{44}$ and $u_0, ..., u_9$ are Galois invariant, we know the linear change of coordinates between them is defined over K. So via this change of coordinates, $A_\epsilon = A$ projectively and $A = t_1 A_\epsilon$ for some $t_1 \in F$. Similarly, $B = t_2 B_\epsilon$ for some $t_2 \in F$. Hence, $t = t_2/t_1 \in F$ satisfies the proposition and is unique.

□

From the proposition above, we can and will always assume we embed J_ϵ in $\mathbb{P}^{15}$ with Galois invariant coordinates $k'_{11}, k'_{12}..., k'_{44}, b'_1, ..., b'_6$. We also know that to compute the twist map $J_\epsilon \subset \mathbb{P}^{15}_{\{k'_{ij}, b'_i\}} \to J \subset \mathbb{P}^{15}_{\{k_{ij}, b_i\}}$, it remains to find the value of $t \in F$ as in Proposition 6.2.5. Because we can always apply a

change of coordinates of J_ϵ over K, it will suffice to find the value of $t \in F$ up to multiplication by an element in K.

Remark 6.2.6. By Remark 1.3.3, we know there are 21 equations vanishing on J of the form $b_i b_j = g_{ij}(k_1, ..., k_4)$, where g_{ij} are quartic forms with coefficients in K. Applying A_ϵ and B_ϵ gives a 21-dimensional F-vector space V of polynomials with coefficients in F. By linear algebra, there exists a unique polynomial in V of the form $b_1^2 - h(k_1, ..., k_4)$ where h is a homogeneous polynomial of degree 4.

Now we prove the following lemma and corollary on computing the value of $t \in F$ as in Proposition 6.2.5 up to scalar multiples in K.

Lemma 6.2.7. *There exist $\lambda, \mu \in F$ and h_1 defined over K such that $h = \lambda h_1 + \mu G_\epsilon$ where h is a homogeneous polynomial of degree 4 defined in Remark 6.2.6 and G_ϵ is the defining equation of the twisted Kummer $\mathcal{K}_\epsilon \subset \mathbb{P}^3_{k_i'}$. Moreover, $\lambda = \lambda_1 \lambda_2^2$ where $\lambda_1 \in K, \lambda_2 \in F$ and λ_1 is unique up to squares in K. In particular, suppose $R \in \mathcal{K}_\epsilon$ is defined over K and let Q denote a preimage of R via the double cover $J_\epsilon \subset \mathbb{P}^{15}_{\{k_{ij}', b_i'\}} \xrightarrow{\theta_\epsilon} \mathcal{K}_\epsilon \subset \mathbb{P}^3_{k_i'}$. Suppose $h_1(R) = h(R) \neq 0$. We have $K(Q) = K(\sqrt{\lambda_1 h_1(R)})$ and Q is defined over K if and only if $\lambda_1 h_1(R)$ is a square in K.*

Proof. By Proposition 6.2.5 and Theorem 1.11.1, we know that $b_1'^2 = g(k_1', ..., k_4')$ where g is homogeneous polynomial of degree 4 and the coefficients of g are defined over K. We observe $h(k_1', ..., k_4') = t^2 g(k_1', ..., k_4')$ on $\mathcal{K}_\epsilon$ with t defined in Proposition 6.2.5. Hence, $\frac{1}{t^2}h - g$ is a degree 4 polynomial vanishing on $\mathcal{K}_\epsilon$. Since the defining equation of $\mathcal{K}_\epsilon$, denoted by G_ϵ, is a irreducible polynomial of degree 4, we get $\frac{1}{t^2}h - g$ is equal to G_ϵ up to scalar multiples in F. Therefore, $h = \lambda h_1 + \mu G_\epsilon$ for some $\lambda, \mu \in F$ and h_1 defined over K.

By the argument above, we have $\frac{1}{t^2}(\lambda h_1 + \mu G_\epsilon) - g$ is equal to G_ϵ up to scalar multiples in F. So $\frac{1}{t^2}\lambda h_1 = g$ on $\mathcal{K}_\epsilon$ which implies that h_1/g is a constant function on $\mathcal{K}_\epsilon$ defined over K. Hence $\frac{1}{t^2}\lambda \in K$ which implies $\lambda = \lambda_1 \lambda_2^2$ for some $\lambda_1 \in K, \lambda_2 \in F$. If we also have $\lambda = \lambda_1' \lambda_2'^2$ for some other $\lambda_1' \in K, \lambda_2' \in F$, then $\lambda_1/\lambda_1' \in K$ is a square in F. This implies λ_1/λ_1' is a square in K as required, as otherwise we get a quadratic sub-extension of K in F which contradicts Proposition 6.2.3(ii).

Finally suppose $R \in \mathcal{K}_\epsilon \subset \mathbb{P}^3_{k_i'}$ is defined over K and $Q \in J_\epsilon \subset \mathbb{P}^{15}_{\{k_{ij}', b_i'\}}$ is a preimage of R via the double cover. By the forms of the 72 defining equations of J_ϵ discussed in Section 1.11, $K(Q) = K(\sqrt{g(R)})$ and Q is defined over K if and only if $g(R)$ is a square in K. But $\frac{1}{t^2}\lambda h_1 = g$ on $\mathcal{K}_\epsilon$ and $\frac{1}{t^2}\lambda = \lambda_1$ up to squares in K. This implies that $K(Q) = K(\sqrt{\lambda_1 h_1(R)})$ and Q is defined over K if and only if $\lambda_1 h_1(R)$ is a square in K as required.

□

Remark 6.2.8. Let $v_1, ..., v_{16}$ be the basis of F as a dimension 16 vector space over K. To solve for $\lambda, \mu \in F$ and h_1 defined over K such that $h = \lambda h_1 + \mu G_\epsilon$, we look for $s_1, ..., s_{16}, t_1, ..., t_{16} \in K$ such that $\sum_{i=1}^{16} s_i v_i G_\epsilon + \sum_{i=1}^{16} t_i v_i h$ has coefficients in K. This is proved to be possible in Lemma 6.2.7.

Corollary 6.2.9. *Suppose $h = \lambda h_1 + \mu G_\epsilon$ as in Lemma 6.2.7 and $\lambda = \lambda_1 \lambda_2^2$ for $\lambda_1 \in K$ and $\lambda_2, \mu \in F$. Then $t = \lambda_2$ up to multiplication in K for the unique t in Proposition 6.2.5.*

Proof. Since for a $t \in F$ that satisfies Proposition 6.2.5, $\frac{1}{t^2}\lambda \in K$ as proved in the proof of Lemma 6.2.7. Hence $(\frac{1}{t}\lambda_2)^2 \in K$ which, by Proposition 6.2.3(ii), implies that $t = \lambda_2$ up to multiplication by an element in K.

□

Suppose $\lambda \in F$ and $K = \mathbb{Q}$. We now describe a practical algorithm in order to solve for λ_1 up to squares satisfying Lemma 6.2.7.

Let $\mathcal{O}_F$ denote the ring of integers of F. We can assume $\lambda \in \mathcal{O}_F$ and $\lambda_1 \in \mathbb{Z}$ square free. It suffices to describe the possible prime factors of λ_1. Suppose $p\mathcal{O}_F = \prod_i v_i^{r_i}$ for v_i primes in $\mathcal{O}_F$. We observe that if $p|\lambda_1$, then $\mathrm{ord}_{v_i}(\lambda) = r_i + 2\,\mathrm{ord}_{v_i}(\lambda_2)$ for all v_i above p, which implies that

$$\mathrm{ord}_{v_i}(\lambda) \equiv r_i \mod 2.$$

We also observe that if $p|\lambda_1$ and $p \nmid N_{F/\mathbb{Q}}(\lambda)$, then $\mathrm{ord}_{v_i}(\lambda_2) = -\frac{r_i}{2} \in \mathbb{Z}$ which implies that r_i is even for any i and p ramifies. Note that we do not need to consider the prime p if p ramifies, $p\mathcal{O}_F = \prod_i v_i^{r_i}$ and $\prod_i v_i^{\frac{r_i}{2}}$ is principal as $\lambda_1\lambda_2^2 = (\frac{\lambda_1}{p})(\nu\lambda_2)^2$ where $\prod_i v_i^{\frac{r_i}{2}} = \nu\mathcal{O}_F$ for some $\nu \in \mathcal{O}_F$. We know that p ramifies if and only if it divides the discriminant of F, denoted by $\triangle_F$, which implies the set of primes that we need to consider is finite and computable.

We summarize the above argument in the short algorithm below.

- Step 1: Scale λ by squares in F such that it is in $\mathcal{O}_F$.
- Step 2: Compute

$$S_1 = \{p \text{ prime} : pO_F = \prod_i v_i^{r_i}, \mathrm{ord}_{v_i}(\lambda) \equiv r_i \bmod 2 \text{ for all } i \text{ and } p|N_{F/\mathbb{Q}}(\lambda)\},$$

$$S_2 = \{p \text{ prime} : pO_F = \prod_i v_i^{r_i}, p|\triangle_F \text{ and } r_i \text{ even for all } i\},$$

$$S_3 = \{p \text{ prime} : p \in S_2 \text{ and } \prod_i v_i^{\frac{r_i}{2}} \text{ is principal}\}.$$

Then $S_1 \cup S_2 \backslash S_3$ gives the set of possible prime factors of λ_1 up to squares satisfying $\lambda = \lambda_1\lambda_2^2$ for some $\lambda_2 \in F$ as in the statement of Lemma 6.2.7.

Remark 6.2.10. In reality, when $K = \mathbb{Q}$, we can always try to use NiceRepresentativeModuloPowers in MAGMA, with details in [Fis08, Section 5]. In the case $K \neq \mathbb{Q}$, we also get a similar computable and finite set of possible places dividing λ_1 which gives a computable and finite set of possible values of λ_1 up to squares as the class group is finite.

6.3 Twist of the Kummer Surface Revisited

As discussed in the previous sections, we will be using the flex algebra method to compute $\mathcal{K}_\epsilon \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ corresponding to ϵ in the general case. Recall the étale algebra $R = \mathrm{Map}_K(J[2], \bar{K})$, defined in Section 3.1.3. From the description of the flex algebra method in Section 3.3.4, we notice that the only non-explicit step is computing the algebras $(R, *_\xi), (R, *_{\xi_\epsilon}), (R, *_\rho)$ as they require computing the trace map defined in Section 3.3.1. In this section, we give an explicit description of the trace map in the general case where $\mathrm{Gal}(f) = S_6$ by Proposition 6.2.1(i). Let $\omega_1, ..., \omega_6$ denote the 6 roots of f and fix P a nontrivial two-torsion point of J corresponding to $\{(\omega_1, 0), (\omega_2, 0)\}$. Define $K_1 := K(P)$. We have K_1 is a degree 15 extension of K and $R \cong K \times K_1$. Recall, the trace map $\mathrm{Tr} : R \otimes R \to R$ is defined via:

$$\mathrm{Tr}(\rho)(T) = \sum_{T_1+T_2=T} \rho(T_1, T_2),$$

and $R \otimes R$ is the étale algebra of Galois equivariant maps from $J[2] \times J[2]$ to $\bar{K}$. The lemma below gives another interpretation of the trace map under the assumptions in this section.

Lemma 6.3.1. *Under the assumptions in this section, we have*

$$R \otimes R \cong K \times K_1 \times K_1 \times K_1 \times M \times N,$$

where M, N are some extensions of K_1 such that $|M/K_1| = 8$ and $|N/K_1| = 6$. Also, the trace map $R \otimes R \to R$ is the same as built out of the trace maps for the constituent fields of $R \otimes R$ and R. More explicitly, under the identifications, $Tr : K \times K_1 \times K_1 \times K_1 \times M \times N \to K \times K_1$ is precisely given by

$$(a, b, c, d, e, f) \mapsto (a + tr_{K_1/K}(d), b + c + tr_{M/K_1}(e) + tr_{N/K_1}(f)),$$

where $tr_{k_2/k_1} : k_2 \to k_1$ denotes the field trace for a finite field extension k_2/k_1.

Proof. Since $\mathrm{Gal}(f) = S_6$, we know $J[2] \times J[2]$ has 6 Galois orbits. The first 4 orbits are $\{(\mathcal{O}_J, \mathcal{O}_J)\}, \{(\mathcal{O}_J, Q), Q \in J[2]\}, \{(Q, \mathcal{O}_J), Q \in J[2]\}, \{(Q, Q), Q \in J[2]\}$. The fifth orbit is the set of pairs (Q_1, Q_2) for $Q_1, Q_2 \in J[2]$ with corresponding Weierstrass points not the same or disjoint and the last orbit is the set of pairs (Q_1, Q_2) for $Q_1, Q_2 \in J[2]$ with disjoint corresponding Weierstrass

points.

Let M denote the field of definition of $(\{(\omega_1,0),(\omega_3,0)\},\{(\omega_2,0),(\omega_3,0)\})$ and N denote the field of definition of $(\{(\omega_3,0),(\omega_4,0)\},\{(\omega_5,0),(\omega_6,0)\})$. Following the proof of Proposition 3.1.10, the isomorphism $R \otimes R \cong K \times K_1 \times K_1 \times K_1 \times M \times N$ is obtained by

$$\rho \mapsto (a,b,c,d,e,f),$$

where $a = \rho(\mathcal{O}_J,\mathcal{O}_J), b = \rho(P,\mathcal{O}_J), c = \rho(\mathcal{O}_J,P), d = \rho(P,P), e = \rho(\{(\omega_1,0),(\omega_3,0)\},\{(\omega_2,0),(\omega_3,0)\}), f = \rho(\{(\omega_3,0),(\omega_4,0)\},\{(\omega_5,0),(\omega_6,0)\})$.

We observe that M, N are extensions of K_1. Since $\mathrm{Gal}(f) = S_6$, we know $\rho(\{(\omega_1,0),(\omega_3)\},\{(\omega_2,0),(\omega_3,0)\}$ has precisely 8 Galois conjugates over K_1 and $\rho(\{(\omega_3,0),(\omega_4,0)\},\{(\omega_5,0),(\omega_6,0)\})$ has 6. Hence $|M/K_1| = 8$ and $|N/K_1| = 6$. More explicitly, $M = K_1(\omega_2,\omega_3)$ and $N = K_1(\omega_3+\omega_4,\omega_3\omega_4)$.

From the definition of the trace map and the definition of the field trace, it can be checked that the corresponding trace map under the identifications: $\mathrm{Tr} : K \times K_1 \times K_1 \times K_1 \times M \times N \to K \times K_1$ is precisely given in the lemma.

□

6.4 Algorithm in Section 5.5.1 Using the Flex Algebra

Recall in Section 5.5.1, we described an algorithm for computing the Cassels-Tate pairing $\langle \epsilon,\eta\rangle_{CT}$ for $\epsilon,\eta \in \mathrm{Sel}^2(J)$, using the formula in Theorem 5.1.1. The algorithm is under the assumption that the twisted Kummer surface $\mathcal{K}_\eta$ has a K-rational point R. Recall the genus two curve $\mathcal{C}$ is defined by $y^2 = f(x)$. As mentioned in the beginning of this chapter, the explicit computation related to ϵ for the Cassels-Tate pairing using this algorithm is done over $L_2 = L_1(\sqrt{a_1},...,\sqrt{a_6})$, where L_1 is the splitting field of $f(x)$ and $(a_1,...,a_6)$ represents the image of ϵ in $L^*/(L^*)^2K^*$ as described in Section 1.10.1 with $L = K[x]/(f)$. In this section, we explain how we can improve the algorithm so that the computation of $\langle \epsilon,\eta\rangle_{CT}$ can potentially be done over a smaller field. Recall we assume we are in the general case where $G_K \xrightarrow{\nu} \mathrm{ASp}_4(\mathbb{F}_2)$ is surjective for all of $\epsilon,\eta,\epsilon+\eta$. This implies the Galois group of $f(x)$ is S_6 and the flex algebras of $\epsilon,\eta,\epsilon+\eta$ are all degree 16 field extensions of K by Proposition 6.2.1(ii). Also although this algorithm works in principle over any number field K, we have only worked out examples when $K = \mathbb{Q}$.

6.4.1 Modifications using the flex algebra method

Start with a genus two curve $\mathcal{C}$ with the following defining equation which we can assume to be defined over $\mathcal{O}_K$ by rescaling y:

$$\mathcal{C} : y^2 = f(x) = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0.$$

We follow the same steps in the algorithm described in Section 5.5.1 with the following modifications.

In the original algorithm, the computation related to $\epsilon \in \mathrm{Sel}^2(J)$ is done using the following commutative diagram:

$$\begin{array}{ccc} J_\epsilon \subset \mathbb{P}^{15} & \longrightarrow & \mathcal{K}_\epsilon \subset \mathbb{P}^3 \\ \downarrow{\scriptstyle \phi_\epsilon} & & \downarrow{\scriptstyle \psi_\epsilon} \\ J \subset \mathbb{P}^{15} & \longrightarrow & \mathcal{K} \subset \mathbb{P}^3, \end{array} \tag{6.4.1}$$

where ϕ_ϵ is computed via the explicit formula in Theorem 1.11.1 and ψ_ϵ is computed via the naive method described in Section 3.2.

In the new algorithm, we compute the commutative diagram (6.4.1) using the isomorphism $\phi_\epsilon : J_\epsilon \subset \mathbb{P}^{15} \to J \subset \mathbb{P}^{15}$ described in Section 6.2.2 and the isomorphism $\psi_\epsilon : \mathcal{K} \subset \mathbb{P}^3 \to \mathcal{K} \subset \mathbb{P}^3$ via the flex algebra method described in Section 3.3. Note that with these modifications to the algorithm, the computation for the Cassels-Tate pairing can be done over a smaller field extension of K comparing to the original algorithm.

Some details and useful techniques

Now we give some details and useful techniques used in the modified algorithm.

(i) We need to make sure the flex algebras of ϵ, η and $\epsilon + \eta$ are indeed isomorphic to degree 16 field extensions of K as required by the algorithm. One method is to find an element in the algebra with minimal polynomial irreducible and degree 16.

(ii) For $\epsilon \in \mathrm{Sel}^2(J)$ represented by (δ, n) as in Remark 1.10.6, we need to solve for $\beta \in L \otimes F = F[x]/(f)$ such that F is the flex algebra of ϵ, $\lambda\beta^2 = \delta \in L$ and $N(\sqrt{\lambda}\beta) = n$. One method is to use MAGMA to find points defined over F of the zero-dimensional variety whose defining equations are obtained by equating $(b_5x^5 + b_4x^4 + ...b_0)^2 = \delta$ up to scaling. As explained in Section 6.2.2, we know this is solvable.

(iii) Suppose $R \in \mathcal{K}_\epsilon(K)$ such that $h(R) \neq 0$ with h defined in Remark 6.2.6. By Section 6.2.2, we can compute a nonzero $a \in K$ such that the preimages of R in J_ϵ are defined over K if and only if a is a square in K. The same method can be used to determine whether a local point on $\mathcal{K}_\epsilon(K_v)$ comes from a local point on $J_\epsilon(K_v)$ for any place v of K. In the case where $h(R) = 0$, we can either look for another $R \in \mathcal{K}_\epsilon(K)$ or change the construction for h via using a polynomial involving b_i^2 with $i \neq 1$ in Remark 6.2.6.

(iv) Let F_1, F_2 and F_3 denote the flex algebras of ϵ, η and $\epsilon + \eta$, respectively. Recall that here we assume all three flex algebras are isomorphic to degree 16 field extensions of K. Suppose we fix embeddings of F_1 and F_2 in $\bar{K}$. Let F_1F_2 denote the composite of F_1 and F_2. We know the images of ϵ, η in $L^*/(L^*)^2K^*$ are represented by $\delta_\epsilon, \delta_\eta$ and $\delta_\epsilon = \lambda_\epsilon\beta_\epsilon^2, \delta_\eta = \lambda_\eta\beta_\eta^2$ for $\lambda_\epsilon \in F_1^*, \lambda_\eta \in F_2^*$ and $\beta_\epsilon \in (L \otimes F_1)^*, \beta_\eta \in (L \otimes F_2)^*$. This implies that the image of $\epsilon + \eta$ in $L^*/(L^*)^2K^*$ is represented by $\delta_\epsilon\delta_\eta = (\lambda_\epsilon\lambda_\eta) \cdot (\beta_\epsilon\beta_\eta)^2$. Viewing $\mathcal{S} \subset \mathbb{P}^5$ as the locus of $(p_0 : ... : p_5)$ for which $P(x)^2$ is congruent to a quadratic in x modulo $f(x)$ and $\mathcal{S}_\epsilon$ as the locus of $(p_0 : ... : p_5)$ for which $\delta_\epsilon P(x)^2$ is congruent to a quadratic in x modulo $f(x)$, we know the twist $\mathcal{S}_\epsilon \to \mathcal{S}$ corresponding to ϵ is the multiplication by β_ϵ and similarly for η. Therefore, if the multiplication by β_ϵ corresponds to the cocycle $(\sigma \mapsto \epsilon_\sigma)$ representing ϵ and the multiplication by β_η corresponds to the cocycle $(\sigma \mapsto \eta_\sigma)$ representing η, then the multiplication by $\beta_\epsilon\beta_\eta$ corresponds to the cocycle $(\sigma \mapsto \epsilon_\sigma + \eta_\epsilon)$ representing $\epsilon + \eta$.

In particular, the field of definition of the coefficient vector of $\beta_\epsilon\beta_\eta$ as a projective point gives an embedding of F_3 in F_1F_2. We note $[F_1F_2 : K] = 256$ by Proposition 6.2.3(ii) and the second isomorphism theorem. Suppose there is another conjugate of F_3, which is $\sigma(F_3)$ for some $\sigma \in G_K$, in F_1F_2. Then there exist $\psi_{\epsilon+\eta}$ defined over F_3 and $\sigma(\psi_{\epsilon+\eta})$ defined over $\sigma(F_3)$ both representing $\epsilon + \eta$. Hence, there exists $P \in J[2]$ such that $\sigma(\psi_{\epsilon+\eta})\psi_{\epsilon+\eta}^{-1}$ is the action of τ_P on $\mathcal{K}$ by Lemma 3.2.2. This implies that there is in fact a unique embedding of F_3 in F_1F_2 because otherwise, there exists a degree 15 subextension of F_1F_2 which is not possible.

(v) In the computation for $\langle \epsilon, \eta \rangle_{CT}$, it is much more practical to first evaluate the $(2, 2, 2)$-form $\mathcal{F}$ following the formula in Corollary 5.2.11 then twist to obtain the quadratic form on $\mathcal{K}_\epsilon$ rather than computing the twisted $(2, 2, 2)$-form $\mathcal{F}_{\epsilon,\eta}$ then evaluate.

6.4.2 Worked example

Now we follow the steps in Section 5.5.1 with the modifications described in Section 6.4.1 and demonstrate with a worked example. In particular, we have chosen an example where computing the Cassels-Tate pairing on $\text{Sel}^2(J)$ does

improve the rank bound obtained via a 2-descent.

Let the genus two curve be given by

$$\mathcal{C} : y^2 = f(x) = -3x^6 + 3x - 15,$$

and define $L = \mathbb{Q}[x]/(f)$. The discriminant of f is $3^{10} \cdot 5^6 \cdot 7 \cdot 31 \cdot 43$. Note that $\mathrm{Gal}(f) = S_6$ as required by the assumptions of this algorithm.

- We pick $\epsilon, \eta \in \mathrm{Sel}^2(J)$ such that the image of ϵ in $L^*/(L^*)^2\mathbb{Q}^*$ is represented by $\delta_\epsilon = -x^5 + 3x^4 + 2x^3 - 5x^2 - 4x + 9$ and the image of η in $L^*/(L^*)^2\mathbb{Q}^*$ is represented by $\delta_\eta = x^5 - 2x^4 + 2x^3 - x^2 + 1$, as given by MAGMA. Moreover, ϵ is represented by $(\delta_\epsilon, -1)$ and η is represented by $(\delta_\eta, 1)$.

- We compute the defining equation G_η for $\mathcal{K}_\eta$ as below

$$\begin{aligned} G_\eta = {} & 18x_1^4 - 44x_1^3x_2 - 4x_1^3x_3 - 192x_1^3x_4 + 128x_1^2x_2^2 - 60x_1^2x_2x_3 + 60x_1^2x_2x_4 \\ & - 472x_1^2x_3^2 + 48x_1^2x_3x_4 + 4x_1^2x_4^2 - 50x_1x_2^3 + 1008x_1x_2^2x_3 - 1316x_1x_2^2x_4 \\ & + 214x_1x_2x_3^2 + 5032x_1x_2x_3x_4 - 1060x_1x_2x_4^2 + 1492x_1x_3^3 + 732x_1x_3^2x_4 \\ & + 948x_1x_3x_4^2 + 748x_1x_4^3 + 300x_2^4 - 486x_2^3x_3 + 1277x_2^3x_4 + 1364x_2^2x_3^2 \\ & + 7457x_2^2x_3x_4 - 4467x_2^2x_4^2 + 1622x_2x_3^3 - 6665x_2x_3^2x_4 + 11222x_2x_3x_4^2 \\ & - 1132x_2x_4^3 + 6280x_3^4 + 25707x_3^3x_4 + 13719x_3^2x_4^2 + 416x_3x_4^3 - 846x_4^4 \end{aligned}$$

  We get a rational point $R = (10 : -24 : -1 : 3)$ on $\mathcal{K}_\eta$ and $a = -3$ where the field of definition of the preimages of R in J_η is $\mathbb{Q}(\sqrt{a})$.

- We compute the defining equation G_ϵ for $\mathcal{K}_\epsilon$ as below

$$\begin{aligned} G_\epsilon = {} & 24389x_1^4 + 95186x_1^3x_2 + 83106x_1^3x_3 - 107648x_1^3x_4 + 226470x_1^2x_2^2 \\ & + 259910x_1^2x_2x_3 - 347912x_1^2x_2x_4 + 35670x_1^2x_3^2 + 281908x_1^2x_3x_4 \\ & + 216612x_1^2x_4^2 - 269094x_1x_2^3 + 54858x_1x_2^2x_3 + 70288x_1x_2^2x_4 \\ & + 159068x_1x_2x_3^2 - 561944x_1x_2x_3x_4 + 516x_1x_2x_4^2 + 47716x_1x_3^3 \\ & + 648048x_1x_3^2x_4 - 304804x_1x_3x_4^2 - 772320x_1x_4^3 + 104621x_2^4 \\ & + 102774x_2^3x_3 - 229260x_2^3x_4 - 32734x_2^2x_3^2 + 674440x_2^2x_3x_4 \\ & + 246364x_2^2x_4^2 + 108444x_2x_3^3 + 1162620x_2x_3^2x_4 - 878172x_2x_3x_4^2 \\ & - 1837912x_2x_4^3 - 212544x_3^4 - 537980x_3^3x_4 + 2226484x_3^2x_4^2 \\ & + 2609168x_3x_4^3 - 3199328x_4^4 \end{aligned}$$

  We compute the rational function g with formula stated in Corollary 5.2.11 and $(c_1, c_2, c_3, c_4) = (1, 0, 0, 0)$, viewed as a rational function on $\mathcal{K}_\epsilon$:

$$g = (2223864x_1^2 + 14731410x_1x_2 + 24847815x_1x_3 - 24788337x_1x_4 + 70375177x_2^2 + 74632289x_2x_3 - 70720951x_2x_4 - 15633788x_3^2 + 80664164x_3x_4 + 58358461x_4^2)/x_1^2$$

- We include some local Cassels-Tate pairing computations. For a place v, we represent a local point on $\mathcal{K}_\epsilon(\mathbb{Q}_v)$ such that the first three coordinates are exact and we give enough precision or decimal places for the last coordinate to pin down a unique point on $\mathcal{K}_\epsilon(\mathbb{Q}_v)$. For a place v, we represent $g(P_v), a$ as elements in $\mathbb{Q}_v^*/(\mathbb{Q}_v^*)^2$.

places v	local points P_v on $\mathcal{K}_\epsilon$	$g(P_v)$	a	$(g(P_v), a)_v$
2	$(0 : 19 : 29 : 5/4 + O(2))$	1	-3	1
3	$(17 : 6 : 11 : 3^4 + O(3^5))$	1	-3	1
5	$(625 : 2 : 18 : 10 + O(5^2))$	1	2	1
7	$(2 : 21 : 10 : 3 \cdot 7^2 + O(7^3)$	-7	1	1
31	$(4 \cdot 31 : 7 : 0 : 410 + O(31^2))$	1	-3	1
43	$(35 \cdot 43 : 13 : 8 : 13 + O(43^2))$	3	-3	1
∞	$(-15 : -7 : 16 : -10.90...)$	-1	-1	-1

- Following the discussion at the end of Section 5.4, we have the following primes that potentially contribute to $\langle \epsilon, \eta \rangle_{CT}$:
  - Prime 2;
  - Prime dividing a: 3;
  - Primes of bad reduction of the genus two curve $\mathcal{C}$: 2, 3, 5, 7, 31, 43;
  - Primes arise from M_ϵ, denoted by S' in Remark 4.4.7(ii): 2, 3, 5, 7, 23, 29, 31, 61, 137, 163, 433, 2423, 2741, 25349, 54319, 62213, 1544864029, 26461826122654523, 2028400254463776241, 530632017512828986501, 33367698266928001452215113524159 41, 46088002934093179647117017920330309 3;
  - Primes below 300.

  It turns out that the only place where the local Cassels-Tate pairing between ϵ and η is non-trivial is ∞ and $\langle \epsilon, \eta \rangle_{CT} = -1$.

Remark 6.4.1. As explained in Remark 5.5.2, we did various sanity checks throughout the computation and suspect that we could reduce the number of primes for the local Cassels-Tate pairing. Since the local pairing is fast to compute even for the largest primes included in this example and primes larger than those, they did not have much effect on the computation. However, it would still be good to find methods to reduce these large primes as factorization will be a problem in larger examples.

Note that in this example, $|\mathrm{Sel}^2(J)| = 2^3$ and $|J(\mathbb{Q})[2]| = 1$. Let r denote the rank of $J(\mathbb{Q})$. The rank bound given by a 2-descent is 3. Recall we have the short exact sequence

$$0 \to J(\mathbb{Q})/2J(\mathbb{Q}) \to \mathrm{Sel}^2(J) \to Ш(A)[2] \to 0.$$

On one hand, we found a rational non-torsion point P on J: $\{(x_1, y_1), (x_2, y_2)\}$ where x_1, x_2 are roots of $x^2 - 119/62x + 199/124$, and $y_i = 7717/1922x_i - 13793/7688$. This implies that $r \geq 1$. Since $|J(\mathbb{Q})/2(J(\mathbb{Q}))| = 2^r \cdot |J(\mathbb{Q})[2]| \geq 2$, we get $|Ш(J)[2]| \leq 2^2$ via the short exact sequence above. On the other hand, $\langle \epsilon, \eta \rangle_{CT} = -1$ which implies that the images of ϵ, η in $H^1(G_K, J)$ are nontrivial elements in $Ш_{nd}(J)[2]$ where $Ш_{nd}(J)$ denotes the quotient of $Ш(J))$ by its maximal divisible subgroup. Note the images of ϵ, η can potentially be the same in $H^1(G_K, J)$. Therefore, if we can show $|Ш_{nd}(J)[2]|$ is a perfect square, then we can deduce that $|Ш_{nd}(J)[2]| = |Ш(J)[2]| = 2^2$. and so $|J(\mathbb{Q})/2(J(\mathbb{Q}))| = 2$ via the short exact sequence above. Hence $r = 1$.

Let $c \in Ш(J)$ denote the class of the principal homogeneous space $\mathrm{Pic}^1(\mathcal{C})$. By [PS99, Theorem 8], we have $|Ш_{nd}(J)[2]|$ is a perfect square if $\langle c, c \rangle_{CT}$ is trivial. Then, from [PS99, Corollary 12], we know that $\langle c, c \rangle_{CT}$ is trivial if and only if the number of *deficient places* of $\mathcal{C}$, defined as places v of $\mathbb{Q}$ such that $\mathcal{C}$ has no $\mathbb{Q}_v$-rational divisor of degree 1, is even. Hence, it suffices to show that the number of deficient places of $\mathcal{C}$ is even.

- p odd and p^3 does not divide the discriminant of f: not deficient. This is because an odd prime p can be deficient only if the discriminant of f is divisible by p^3 by [PS99, Lemma 18]. Recall the discriminant of f is $3^{10} \cdot 5^6 \cdot 7 \cdot 31 \cdot 43$.

- $p = 5$: $x = 2, y = 2$ is a smooth point on $\bar{\mathcal{C}}(\mathbb{F}_5)$. Then by Hensel's Lemma, $\#\mathcal{C}(\mathbb{Q}_5) > 0$ which implies that 5 is not a deficient place.

- $p = 2$: We note that $y^2 = -3x^6 + 3x - 15$ has a solution over $\mathbb{Z}_2$ when $x = 0$, as $-15 \equiv 1(8)$.

- $p = 3$: By [PS99, Lemma 16], we know that an odd prime p is deficient if $f(x) = uh(x)^2 + pj(x)$ where the reduction of $u \in \mathbb{Z}_p$ is in $\mathbb{F}_p^* \setminus (\mathbb{F}_p^*)^2$, $\deg h = 3, \deg j = 6$ and if the reductions of h, j modulo p have no common factor of odd degree. Since we can write $f(x) = -(3x^3)^2 + 3(-x^6 + x - 5 + 3x^6)$ and it can be checked that $-x^6 + x - 5$ is irreducible modulo 3, we get $p = 3$ is deficient.

- ∞: It can be checked that $-3(x^6 - x + 5) < 0$ for any $x \in \mathbb{R}$ which implies that $\mathcal{C}(\mathbb{R}) = \emptyset$. Suppose D is a $\mathbb{R}$-divisor of degree 1 on $\mathcal{C}$, then

$D = D_1 - D_2$, for some D_1, D_2 effective divisors with disjoint support. In particular, D_1, D_2 are $\mathbb{R}$-divisors and the degree of precisely one of them is odd. This gives a contradiction as $\mathcal{C}(\mathbb{R}) = \emptyset$ and any effective $\mathbb{R}$-divisor on $\mathcal{C}$ is a sum of complex conjugate pairs. So ∞ is a deficient place.

Note, the computation of the deficient places for genus two curves defined over $\mathbb{Q}$ is implemented in MAGMA and we have verified our results.

We also observe that without computing the Cassels-Tate pairing, we only know $r = 1, 2$ or 3 by carrying out a 2-descent, finding a rational non-torsion point on J and computing the number of deficient places.

Bibliography

[AS02] A. Agashe and W. Stein, *Visibility of Shafarevich–Tate Groups of Abelian Varieties*, Journal of Number Theory **97** (2002), no. 1, 171-185, DOI 10.1006/jnth.2002.2810. ↑

[vB] M. van Beek, *Computing the Cassels-Tate Pairing*. Doctoral Dissertation. University of Cambridge, 2015. ↑

[vBF18] M. van Beek and T. A. Fisher, *Computing the Cassels-Tate pairing on 3-isogeny Selmer groups via cubic norm equations*, Acta Arithmetica **185** (2018), no. 4, 367-396, DOI 10.4064/AA171108-11-4. ↑

[BL04] C. Birkenhake and H. Lange, *Complex Abelian Varieties*, Grundlehren der mathematischen Wissenschaften, vol. 302, Springer-Verlag Berlin Heidelberg, 2004. ↑

[Bli14] H.F. Blichfeldt, *A new principle in the geometry of numbers, with some applications*, Transactions of the American Mathematical Society **15** (1914), no. 3, 227–235. ↑

[BD11] N. Bruin and K. Doerksen, *The Arithmetic of Genus Two Curves with (4, 4)-Split Jacobians*, Canadian Journal of Mathematics **63** (2011), no. 5, 992-1024, DOI 10.4153/CJM-2011-039-3. ↑

[Cas59] J. W. S. Cassels, *Arithmetic on Curves of Genus 1. I. On a conjecture of Selmer.*, Journal für die reine und angewandte Mathematik **202** (1959), 52-99. ↑

[Cas62] ———, *J. W. S. Cassels, Arithmetic on curves of genus 1, IV. Proof of the Hauptvermutung.*, Journal für die reine und angewandte Mathematik **211** (1962), 95-112, DOI 10.1515/crll.1962.211.95. ↑

[Cas98] ———, *Second Descents for Elliptic Curves*, Journal für die reine und angewandte Mathematik **494** (1998), 101-127, DOI 10.1515/crll.1998.001. ↑

[CF96] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a MiddleBrow Arithmetic of Curves of Genus 2*, London Mathematical Society Lecture Note Series, vol. 230, Cambridge University Press, 1996. ↑

[CF67] J. W. S. Cassels and A. Frohlich, *Algebraic Number Theory*, Proceedings of an instructional conference organized by the London Mathematical Society (a nano advanced study institute) with the support of the international union, Academic Press Inc. (London) LTD., 1967. ↑

[Cla05] P. L. Clark, *The Period–Index Problem in WC-Groups I: Elliptic Curves*, Journal of Number Theory **114** (2005), no. 1, 193-208, DOI 10.1016/j.jnt.2004.10.001. ↑

[CM96] D. Coray and C. Manoil, *On large Picard groups and the Hasse Principle for curves and K3 surfaces*, Acta Arithmetica **76** (1996), no. 2, 165-189, DOI 10.4064/aa-76-2-165-189. ↑

[CFO+08] J.E. Cremona, T.A. Fisher, C. O'Neil, D. Simon, and M. Stoll, *Explicit n-Descent on Elliptic Curves I. Algebra*, Journal für die reine und angewandte Mathematiks **615** (2008), 121-155, DOI 10.1515/CRELLE.2008.012. ↑

[CFO+15] ———, *Explicit n-Descent on Elliptic Curves III. Algorithms*, Math. Comp **84** (2015), 895-922, DOI 10.1090/S0025-5718-2014-02858-5. MR3290968 ↑

[CR03] J.E. Cremona and D. Rusin, *Efficient Solutions of Rational Conics*, Math. Comp. **72** (2003), no. 243, 1417–1441, DOI 10.1090/S0025-5718-02-01480-1. ↑

[Don15] S. Donnelly, *Algorithms for the Cassels-Tate pairing* (2015). preprint. ↑

[Fis03] T. A. Fisher, *The Cassels–Tate pairing and the Platonic solids*, Journal of Number Theory **98** (2003), no. 1, 105-155, DOI 10.1016/S0022-314X(02)00038-0. ↑

[Fis08] ———, *Some Improvements to 4-Descent on an Elliptic Curve*, International Algorithmic Number Theory Symposium, posted on 2008, 125-138, DOI 10.1007/978-3-540-79456-1-8. ↑

[Fis16] ———, *On binary quartics and the Cassels-Tate pairing* (2016). preprint. ↑

[FN14] T. A. Fisher and R. Newton, *Computing the Cassels-Tate pairing on the 3-Selmer group of an elliptic curve*, Journal of Number Theory **10** (2014), no. 7, 18811907, DOI 10.1142/S1793042114500602. ↑

[FSS10] T. A. Fisher, E. F. Schaefer, and M. Stoll, *The Yoga of the Cassels-Tate Pairing*, LMS Journal of Computation and Mathematics **13** (2010), 451 - 460, DOI 10.1112/S1461157010000185. ↑

[Fla90] M. Flach, *A generalisation of the Cassel-Tate pairing*, Journal für die reine und angewandte Mathematik **412** (1990), 113-127. ↑

[Fly90] E. V. Flynn, *The Jacobian and Formal Group of a Curve of Genus 2 over an Arbitrary Ground Field*, Mathematical Proceedings of the Cambridge Philosophical Society **107** (1990), no. 3, 425-441, DOI 10.1017/S0305004100068729. ↑

[Fly93] ———, *The Group Law on the Jacobian of a Curve of Genus 2*, Journal für die reine und angewandte Mathematik **439** (1993), 45-70. ↑

[Fly18] ———, *Arbitrarily Large Tate–Shafarevich Group on Abelian Surfaces*, Journal of Number Theory **186** (2018), 248-258, DOI 10.1016/j.jnt.2017.10.004. ↑

[FTvL12] E. V. Flynn, D. Testa, and R. van Luijk, *Two-Coverings of Jacobians of Curves of Genus 2*, Proceedings of the London Mathematical Society **104** (2012), no. 2, 387–429, DOI 10.1112/plms/pdr012. ↑

[Fri] C. Friedrichs, *Berechnung von Maximalordnungen uber Dedekindringen*. Dissertation, Technische Universit at Berlin, 2000, http://opus.kobv.de/tuberlin/volltexte/2001/40/pdf/friedrichs carsten.pdf. ↑

[GS06] P. Gille and T. Szamuely, *Central Simple Algebras and Galois Cohomology*, Cambridge Studies in Advanced Mathematics, vol. 101, Cambridge University Press, 2006. ↑

[IR93] G. Ivanyos and L. R'onyai, *Finding maximal orders in semisimple algebras over Q*, Computational Complexity **3** (1993), 245–261. ↑

[IRS12] G. Ivanyos, L. R'onyai, and J. Schicho, *Splitting full matrix algebras over algebraic number fields*, Journal of Algebra **354** (2012), no. 1, 211-223. ↑

[IS96] G. Ivanyos and A. Szanto, *Lattice basis reduction for indefinite forms and an application*, Discrete Mathematics **153** (1996), no. 1-3, 177-188, DOI 10.1016/0012-365X(95)00135-J. ↑

[Har77] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, vol. 52, Springer, New York, NY, 1977. ↑

[HS00] M. Hindry and J. H. Silverman, *Diophantine Geometry: An Introduction*, Graduate Texts in Mathematics 201, vol. 52, Springer, 2000. ↑

[Lan56] S. Lang, *Algebraic Groups Over Finite Fields*, American Journal of Mathematics **78** (1956), no. 3, 555-563, DOI 10.2307/2372673. ↑

[LT58] S. Lang and J. Tate, *Principal Homogeneous Spaces Over Abelian Varieties*, American Journal of Mathematics **80** (1958), no. 3, 659-684, DOI 10.2307/2372778. ↑

[LLL82] A. K Lenstra, H. W. Lenstra, and L. Lovász, *Factoring polynomials with rational coefficients*, Mathematische Annalen **261** (1982), 515–534, DOI 10.1007/BF01457454. ↑

[Mil86] J.S. Milne, *Abelian Varieties*, Springer, New York, 1986. pp 103-150 of Arithmetic Geometry. ↑

[Mil06] ———, *Arithmetic Duality Theorems, Second Edition*, BookSurge, LLC, 2006. ↑

[Mil08] ———, *Abelian Varieties, Second Edition*, 2008. Available at www.jmilne.org/math/. ↑

[Mum69] D. Mumford, *Varieties Defined by Quadratic Equations. 1970 Questions on Algebraic Varieties (C.I.M.E., III Ciclo*, Varenna (1969), 29-100. ↑

[Mum70] ———, *Abelian Varieties*, Tata Institute of Fundamental Research Studies in Mathematics, Oxford University Press, 1970. Published for the Tata Institute of Fundamental Research, Bombay. ↑

[O'N02] C. O'Neil, *The Period-Index Obstruction for Elliptic Curves*, Journal of Number Theory **95** (2002), no. 2, 329-339, DOI 10.1006/jnth.2001.2770. ↑

[PP04] G. Pareschi and M. Popa, *Regularity on Abelian Varieties II: Basic Results on Linear Series and Defining Equations*, J. Algebraic Geom. **13** (2004), 167-193, DOI 10.1090/S1056-3911-03-00345-X. MR2008719 ↑

[Pil07] J. Pilnikova, *Trivializing a Central Simple Algebra of Degree 4 over the Rational Numbers*, Journal of Symbolic Computation **42** (2007), no. 6, 579-586, DOI 10.1016/j.jsc.2007.01.001. ↑

[PS97] B. Poonen and E. F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. **488** (1997), 141–188. ↑

[PS99] B. Poonen and M. Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Annals of Mathematics **150** (1999), no. 3, 1109-1149, DOI 10.2307/121064<. MR1740984 ↑

[Rei03] I. Reiner, *Maximal orders*, LMS Monographs, New Series 28, Oxford University Press, 2003. ↑

[R'o90] L. R'onyai, *Computing the structure of finite algebras*, Journal of Symbolic Computation **9** (1990), no. 3, 355–373, DOI 10.1016/S0747-7171(08)80017-X. ↑

[Sch95] E. F. Schaefer, *2-Descent on the Jacobians of Hyperelliptic Curves*, Journal of Number Theory **51** (1995), no. 2, 219-232, DOI 10.1006/jnth.1995.1044. ↑

[Ser79] Jean-Pierre Serre, *Local Fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag New York, 1979. ↑

[Ser97] ———, *Galois Cohomology*, Springer Monographs in Mathematics, Springer-Verlag Berlin Heidelberg, 1997. ↑

[Sha59] I.R. Shafarevich, *The Group of Principal Homogeneous Algebraic Manifolds*, Doklady Akademii Nauk SSS **124** (1959), 42-43. ↑

[Sim05] D. Simon, *Solving Quadratic Equations Using Reduced Unimodular Quadratic Forms*, Math. of Comp **74** (2005), no. 251, 1531–1543. ↑

[Sko] A. Skorobogatov, *Abelian varieties over local and global fields*. TCC course, Spring 2016. ↑

[TY09] K. Takashima and R. Yoshida, *An algorithm for computing a sequence of Richelot isogenies*, Bulletin of the Korean Mathematical Society **46** (2009), no. 4, 789-802, DOI 10.4134/BKMS.2009.46.4.789. ↑

[Tat62] J. Tate, *Duality theorems in Galois cohomology over number fields*, Proc. In- ternat. Congr. Mathematicians (Stockholm) (1962), 288–295. Inst. Mittag-Leffler, Djursholm (1963). ↑

[Voi05] J. Voight, *Quadratic forms and quaternion algebras: algorithms and arithmetic* (2005). Ph.D. thesis, University of California, Berkeley, CA. ↑

[Voi14] ———, *The Arithmetic of Quaternion algebras* (2014). Available in the author's website: https://math.dartmouth.edu/ jvoight/articles/quat-book-052714.pdf. ↑